7108500923

FAST®

制 造 商：深圳市友佳联科技有限公司
公司地址：深圳市南山区留仙大道红花岭
工业区二区三栋四层
网 址：http://www.fastcom.com.cn

FAST®

迅捷FR516/FR524

多 端 口 企 业 宽 带 路 由 器

用 户 手 册

Rev: 1.0.2

声 明

本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。除非有特殊约定，本手册仅作为使用指导，本手册中的所有陈述、信息等均不构成任何形式的担保。



网址：www.fastcom.com.cn

技术支持热线：400-8830-660

技术支持E-mail：fae@fastcom.com.cn

公司地址：深圳市南山区留仙大道红花岭工业区二区三栋四层

邮编：518055

目 录

物 品 清 单

请您小心打开包装盒，里面应有以下配件:

- 一台多端口企业宽带路由器
- 一根电源线
- 一本用户手册
- 一张保修卡

如果发现有配件短缺或损坏的情况，请及时和当地经销商联系。

第1章 用 户 手 册 简 介

首先感谢您购买 FR516/FR524 多端口企业宽带路由器! FR516/FR524 多端口企业宽带路由器是专为满足小型企业、网吧用户需求而设计的，它集高性能、高安全、多管理功能于一身，为您提供高价值的网络连接。它配置简单，无需专业人员即可按照本手册安装配置。

在您准备安装使用本产品之前，请先仔细阅读本手册，以便全面利用本产品的所有功能。

1.1 用途

本手册的用途是帮助您熟悉和正确使用 FR516/FR524 多端口企业宽带路由器。

1.2 约定

本手册中所提到的路由器，如无特别说明，系指FR516/FR524多端口企业宽带路由器，下面简称为FR516/FR524。

本手册采用的图片中都配有相关参数，实际产品的配置界面并没有提供，这些参数主要是为您正确设置参数提供参考，您可以根据实际需要选择是否设置或修改这些参数。

1.3 用户手册概述

第 1 章：用户手册简介。

第 2 章：产品概述——简述路由器的主要特性和规格。

第 3 章：硬件安装——帮助您进行路由器的硬件安装。

第 4 章：快速安装指南——帮助您配置路由器的基本网络参数。

第 5 章：配置指南——帮助您配置路由器的高级特性。

附 录 A：FAQ。

附 录 B：IE 浏览器设置。

第2章 产 品 概 述

2.1 产 品 简 介

FR516/FR524多端口企业宽带路由器是专为渴望实现高速上网、方便管理的经济型SOHO(小型办公室和家庭办公室)用户设计，功能实用、易于管理。

FR516/FR524多端口企业宽带路由器提供多方面的管理功能，可以对DHCP、DMZ主机、虚拟服务器、防火墙等进行管理；能够组建内部局域网，允许多台计算机共享一条单独宽带线路和ISP账号，并提供自动或按时连通和断开网络连接功能，节省用户上网费用；特有的防火墙功能，可以有效控制内网用户的上网权限，过滤不良网站。

FR516/FR524 多端口企业宽带路由器安装和配置简单。采用全中文的配置界面，每步操作都配有详细的帮助说明。特有的快速配置向导更能帮您轻松快速地实现网络连接。

2.2 特 性 和 规 格 说 明

2.2.1 主要特性

- 提供一个10/100M以太网(WAN)接口，可接xDSL Modem/Cable Modem/Ethernet
- FR516内部集成16口交换机，提供16个10/100M以太网(LAN)接口，10/100Mbps自适应，支持端口自动翻转（Auto MDI/MDIX）
- FR524内部集成24口交换机，提供24个10/100M以太网(LAN)接口，10/100Mbps自适应，支持端口自动翻转（Auto MDI/MDIX）
- 内置网络地址转换(NAT)功能，支持虚拟服务器、特殊应用程序和DMZ主机
- 内建DHCP服务器，同时可进行静态地址分配
- 支持VPN Pass-through，可以构建VPN客户端
- 支持通用即插即用(UPnP)，符合UPnP标准的数据可顺利通过
- 内置防火墙功能，支持域名过滤和MAC地址过滤，可以有针对地开放指定计算机的上网权限
- 支持IP与MAC绑定功能，可以有效防止网络攻击

- 支持动态DNS功能，能够为动态IP地址提供域名服务
- 内置静态路由功能，可以根据需要构建特殊网络拓扑
- 支持WEB软件升级，可以免费获得路由器的最新软件
- 可以根据上网动作，自动或按时连通和断开网络连接
- 支持远程和Web管理，全中文配置界面，配备简易安装向导(Wizard)

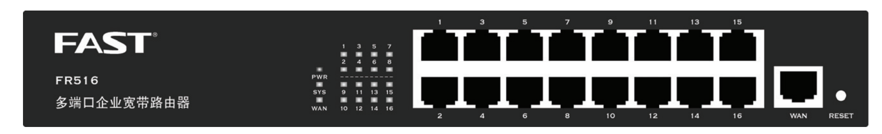
2.2.2 规格

支持的标准和协议		IEEE 802.3、IEEE 802.3u、IEEE 802.3x、TCP/IP、DHCP、ICMP、NAT、PPPoE、SNTP
端口	LAN口	16/24个10/100M自适应RJ45端口(Auto MDI/MDIX)
	WAN口	1个10/100M自适应RJ45端口(Auto MDI/MDIX)
网络介质		10Base-T：3类或3类以上UTP
		100Base-TX：5类UTP
LED指示	端口	LAN(1~16，1~24)，WAN(指示各端口的Link/Act状态)
	其它	SYS(系统状态指示灯)，PWR（电源状态指示灯）
外形尺寸(L x W x H)		294mm x 180mm x 44mm
使用环境		工作温度：0ºC - 40ºC
		存储温度：-40ºC - 70ºC
		工作湿度：10% - 90% RH不凝结
		存储湿度：5% - 90% RH不凝结
电源及功耗		FR516：输入：220V AC, 50Hz，0.1A 功耗：最大11W
		FR524：输入：100-240V AC，50/60Hz，0.6A 功耗：最大11W

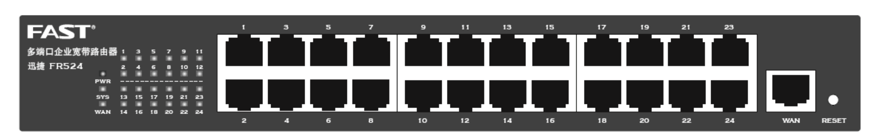
第3章 硬件安装

3.1 面板布置

3.1.1 前面板



FR516前面板图



FR524前面板图

➢ 指示灯:

指示灯	说明	描述	备注
PWR	电源状态指示灯	常灭－电源输入不正常或无输入 常亮－电源输入正常	
SYS	系统状态指示灯	常灭－系统存在故障 常亮－系统初始化故障 闪烁－系统正常	SYS 灯快闪数次表示正在恢复出厂设置
1~16 1~24	局域网状态指示灯	常灭－相应端口没有连接上 常亮－相应端口已正常连接 闪烁－相应端口正在进行数据传输	
WAN	广域网状态指示灯	常灭－端口没有连接上 常亮－端口已正常连接 闪烁－端口正在进行数据传输	

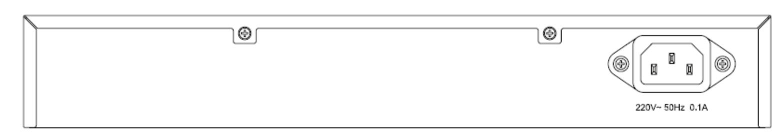
➢ **WAN**: 1 个广域网端口(RJ45)。连接 xDSL/Cable Modem 或以太网。

➢ **LAN**: FR516/FR524 提供 16/24 个局域网端口(RJ45)，计算机、集线器/交换机等通过这些端口连入局域网。

- **Reset：**复位按钮。在工作状态下，连续按住 **Reset** 键 5 秒，system 灯快闪，即可恢复到出厂默认值。

⚠ 注意：在路由器未完全启动前，不能关闭电源，否则，配置有可能没有恢复到出厂默认值。

3.1.2 后面板



FR516后面板图



FR524后面板图

- **电源插孔：**这个插孔供您插接电源。

⚠ 注意：FR516 的电源规格为：220V AC，50Hz；FR524 的电源规格为：100-240V AC，50/60Hz，如果使用不匹配的电源，可能会导致路由器损坏。

3.2 系统需求

- 宽带 Internet 服务（接入方式为 xDSL/Cable Modem 或以太网）
- 具有以太网 RJ45 连接器的调制解调器（直接接入以太网时不需要此物件）
- 每台 PC 的以太网连接（网卡和网线）
- TCP/IP 网络软件（Windows 95/98/ME/NT/2000/2003/XP/Vista 自带）
- Internet Explorer 5.0 或更高版本

3.3 安装环境

安装环境要求：

- 将路由器水平放置
- 尽量将路由器放置在远离发热器件处
- 不要将路由器置于太脏或潮湿的地方

路由器推荐使用环境:

- 温度：0 ºC ~ 40 ºC
- 湿度：10% ~ 90%RH，无凝结

3.4 硬件安装步骤

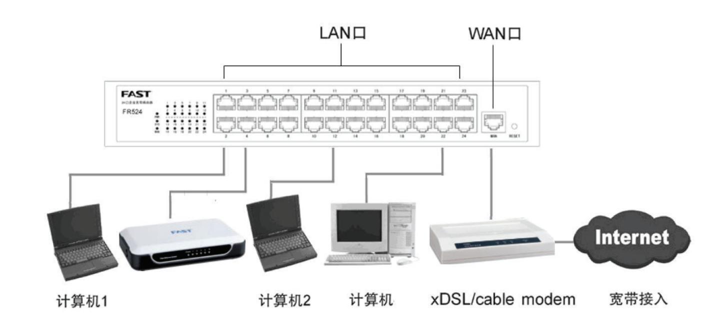
在安装路由器前，我们希望您已经能够利用您的宽带服务在单台计算机上成功上网。如果您单台计算机上宽带网有问题，请先和您的网络服务商（ISP）联系解决问题。当您成功地利用单台计算机上网后，请遵循以下步骤安装您的路由器。切记安装时拔除电源插头，保持双手干燥。

1）建立局域网连接

用一根网线连接路由器的 LAN 口和局域网中的集线器或交换机，如下图所示（以 FR524 为例）。您也可以用一根网线将路由器与您的计算机网卡直接相连。

2）建立广域网连接

用网线连接路由器和 xDSL/Cable Modem 或以太网，如下图所示（以 FR524 为例）。



3）连接电源

将电源连接好，路由器将自行启动。

本产品专为通信运营商管理的机房使用设计，请按以上提示进行安装维护。

第4章 快速安装指南

要正确使用路由器，您必须合理配置网络。下面以 Windows XP 为例，讲述具体配置过程。如果只进行基本配置，您只需阅读本章内容；如果要进行高级配置，请继续阅读第五章内容。

4.1 建立正确的网络设置

路由器默认 IP 地址是 192.168.1.1，默认子网掩码是 255.255.255.0。这些值可以根据您的实际需要而改变，但本用户手册上将按默认值说明。

首先请将您的计算机接到路由器的局域网端口，接下来您可以使用两种方法为您的计算机设置 IP 地址。

➢ **方法一**：**手动设置 IP 地址。**

- 设置您计算机的 TCP/IP 协议。如果您已经正确设置完成，请跳过第一步。
- 设置您计算机的 IP 地址为 192.168.1.xxx（xxx 范围是 2 至 254），子网掩码为 255.255.255.0，默认网关为 192.168.1.1。

➢ **方法二**：**利用路由器内置 DHCP 服务器自动设置 IP 地址。**

- 设置您计算机的 TCP/IP 协议为"自动获取 IP 地址"。
- 这样路由器内置 DHCP 服务器将自动为您的计算机设置 IP 地址。



注意：Windows 98 或更早版本的操作系统，以上设置可能需要重启您的计算机。

在设置好 TCP/IP 协议后，您可以使用 Ping 命令检查您的计算机和路由器之间是否联通。下面的例子为一个在 Windows XP 环境中，执行 Ping 命令，操作步骤如下:

首先请您点击桌面的"开始"菜单，再选择"运行"选项，并在随后出现的运行输入框内输入 cmd 命令，然后回车或点击"确认"键即可进入下图所示界面。

最后在该界面中输入命令 Ping 192.168.1.1，其结果显示如下。

如果屏幕显示为:

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

那么恭喜您！您的计算机已与路由器成功建立连接。如果屏幕显示为:

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

这说明设备还未安装好，您可以按照下列顺序检查:

1) 硬件连接是否正确?

提示: 路由器面板上对应局域网端口的 Link/Act 指示灯和您计算机上的网卡灯必须亮。

2) 您的计算机的 TCP/IP 设置是否正确?

提示: 如果路由器的 IP 地址为 192.168.1.1，那么您的计算机 IP 地址必须为 192.168. 1.xxx（xxx 范围是 2~254）。

4.2 快速安装指南

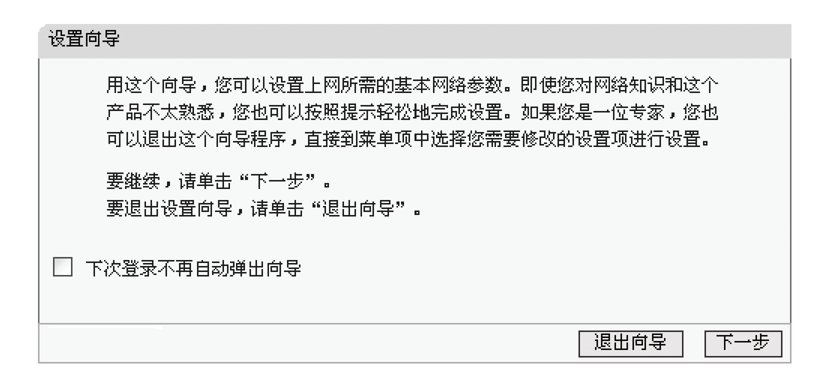
本产品提供基于浏览器（Internet Explorer 或 Netscape Communicator）的配置界面，这种配置方案适宜于任何 MS Windows，Macintosh 或 UNIX 平台。

激活浏览器，取消"使用代理服务器"选项或者将路由器的 IP 地址添加到"代理服务器设置"中的"例外"栏中（在 IE 中选择"工具－Internet 选项－连接－局域网设置"，就可以找到这些设置）。接着在浏览器的地址栏里输入路由器的 IP 地址，例如 http://192.168.1.1。

连接建立起来后，您将会看到下图所示登录界面。您需要以系统管理员的身份登录，即在该登录界面输入用户名和密码（用户名和密码的出厂设置均为“admin”），然后单击确定按钮。



如果名称和密码正确，浏览器将显示管理员模式的画面，并会弹出一个设置向导的画面（如果没有自动弹出的话，可以单击管理员模式画面左边“设置向导”菜单将它激活）。



单击“下一步”，进入上网方式选择画面。

设置向导

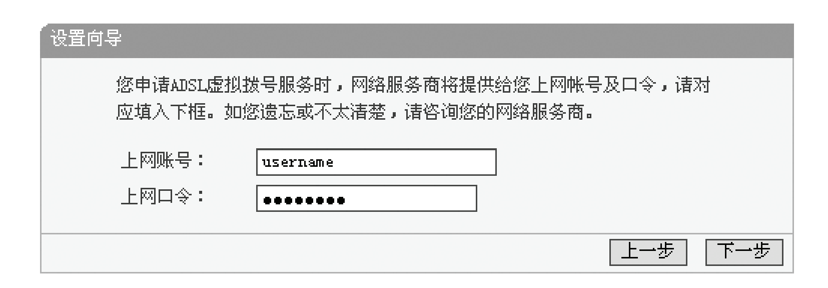
本路由器支持三种常用的上网方式，请您根据自身情况进行选择。

◯ ADSL虚拟拨号（PPPoE）
◉ 以太网宽带 ，自动从网络服务商获取IP地址（动态IP）
◯ 以太网宽带 ，网络服务商提供的固定IP地址（静态IP）

上一步　下一步

以上画面显示了最常用的三种上网方式，您可以根据自身情况进行选择，然后单 击“下一步”填写上网所需的基本网络参数。

1) 如果您的上网方式为 PPPoE，即 ADSL 虚拟拨号方式，则您需要填写以下内容:



- **上网帐号**: 填入 ISP 为您指定的 ADSL 上网帐号，不清楚可以向 ISP 询问。
- **上网口令**: 填入 ISP 为您指定的 ADSL 上网口令，不清楚可以向 ISP 询问。

2) 如果您的上网方式为动态 IP，即您可以自动从网络服务商获取 IP 地址，则您不需要填写任何内容即可直接上网。

3) 如果您的上网方式为静态 IP，即您拥有网络服务商提供的固定 IP 地址，则您需要填写以下内容:

设置向导-静态IP

您申请以太网宽带服务，并具有固定IP地址时，网络服务商将提供给您一些基本的网络参数，请对应填入下框。如您遗忘或不太清楚，请咨询您的网络服务商。

IP地址：	222.88.88.222	
子网掩码：	255.255.255.0	
网关：		（可选）
DNS服务器：		（可选）
备用DNS服务器：		（可选）

帮 助　　上一步　下一步

- **IP 地址**：本路由器对广域网的 IP 地址，即 ISP 提供给您的 IP 地址，不清楚可以向 ISP 询问。
- **子网掩码**：本路由器对广域网的子网掩码，即 ISP 提供给您的子网掩码，一般为 255.255.255.0。
- **网关**：填入 ISP 提供给您的网关，不清楚可以向 ISP 询问。
- **DNS 服务器**：填入 ISP 提供给您的 DNS 服务器地址，不清楚可以向 ISP 询问。
- **备用 DNS 服务器**：可选项，如果 ISP 提供给您了两个 DNS 服务器地址，则您可以 把另一个 DNS 服务器地址的 IP 地址填于此处。

在填写完上网所需的基本网络参数之后，会出现设置向导完成界面。

设置向导

恭喜您！您已经顺利完成上网所需的基本网络参数的设置，现在您已经能够正常上网。

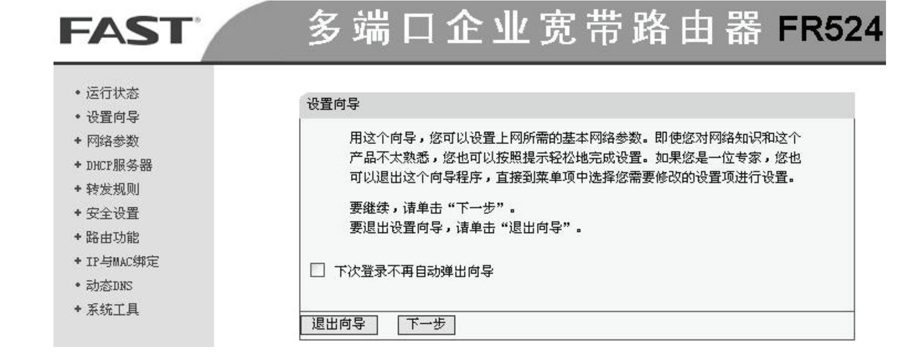
请单击“完成”结束设置向导。

返 回　完 成

第5章　配置指南

5.1 启动和登录

在启动和登录成功以后，浏览器会显示管理员模式下的路由器配置页面(以FR524 为例)。



在左侧菜单栏中，共有"运行状态"、"设置向导"、"网络参数"、"DHCP 服务器"、"转发规则"、"安全设置"、"路由功能"、"IP 与 MAC 绑定"、"动态 DNS"、和"系统工具"十个菜单。单击某个菜单项，您即可进行相应的功能设置。

在使用过程中，如果您对本产品的功能有任何疑问，您只需单击该页面的"帮助"按钮，即可获得详细的联机帮助。

下面将详细讲解各个菜单的功能。

5.2 运行状态

版本信息

当前软件版本：	3.6.1 Build 080311 Rel.34295na
当前硬件版本：	FR524 1.0 10C2225B

LAN口状态

MAC 地址：	00-0A-EB-EA-27-F1
IP地址：	192.168.1.2
子网掩码：	255.255.255.0

WAN口状态

MAC 地址：	00-0A-EB-EA-27-F2	
IP地址：	10.20.1.186	静态IP
子网掩码：	255.255.255.0	
网关：	10.20.1.254	
DNS 服务器：	10.20.1.254 , 0.0.0.0	

WAN口流量统计

	接收	发送
字节数：	0	0
数据包数：	0	10

运行时间： 0 day(s) 00:02:05 [刷 新]

本页显示路由器的工作状态。

1) 版本信息

此处显示当前的软、硬件版本。

2) **LAN** 口状态

此处显示当前 LAN 口的 MAC 地址、IP 地址和子网掩码。

3) **WAN** 口状态

此处显示 WAN 口的 MAC 地址、IP 地址、子网掩码、网关和 DNS 服务器。同时 IP 地址右侧将显示用户上网方式（PPPoE/动态 IP/静态 IP）。如果用户的上网方式为 PPPoE（ADSL 拨号上网）的话，当用户已经连接上 Internet 时，此处将会显示用户的上网时间和"断线"按钮，单击此按钮可以进行即时的断线操作，当用户未连接 Internet 时，此处将会显示"连接"按钮，单击此按钮可以进行即时的连接操作。

4) WAN 口流量统计

此处显示 WAN 口接收和发送的数据流量信息。

⚠ **注意:**

在 IP 地址右侧会显示用户的上网方式(动态 IP/静态 IP/PPPoE/802.1X+动态 IP/802.1X+静态 IP/L2TP/PPTP)。当用户的上网方式为 PPPoE、L2TP、PPTP(ADSL 拨号上网)，并且用户已经连接上 Internet 时，此处将会显示用户的上网时间和断线按钮，单击此按钮可以进行即时的断线操作；如果用户尚未连接 Internet 时，此处将会显示连接按钮，单击此按钮可以进行即时的连接操作。

5.3 设置向导

请参考第 4 章的快速安装指南。

5.4 网络参数

选择菜单网络参数，您可以看到:

- 网络参数
  - LAN口设置
  - WAN口设置
  - MAC地址克隆
  - WAN端口参数

单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.4.1 LAN口设置

选择菜单**网络参数→LAN口设置**，您可以在下图1界面中配置LAN接口的网络参数。如果需要，可以更改LAN接口IP地址以配合实际网络环境的需要。

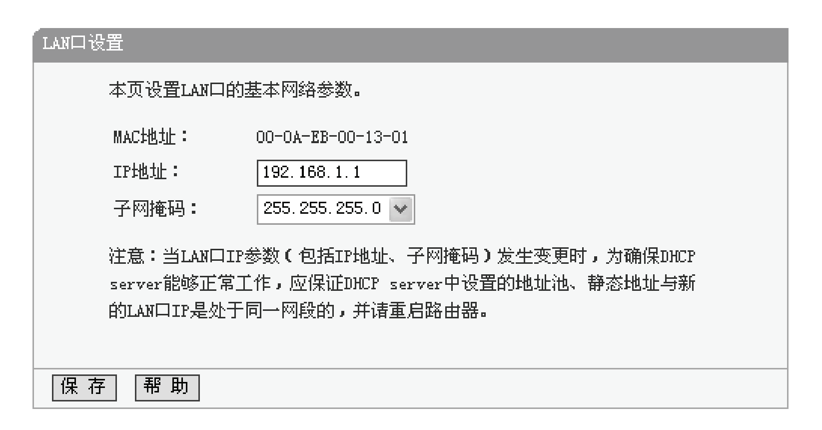


图 1 LAN 口设置

- MAC地址：本路由器对局域网的MAC地址，用来标识局域网，不可更改。
- IP地址：本路由器对局域网的IP地址。该IP地址出厂默认值为192.168.1.1，您可以根据需要改变它。
- 子网掩码：本路由器对局域网的子网掩码，可以在下拉列表中选择B类(255.255.0.0)或者C类(255.255.255.0)地址的子网掩码。一般情况下选择255.255.255.0即可。

完成更改后，点击**保存**按钮，路由器会自动重启。

注意:

1) 如果改变了本地IP地址，您必须用新的IP地址才能登录路由器的WEB管理界面，并且局域网中所有计算机的默认网关必须设置为该IP地址才能正常上网。
2) 局域网中所有计算机的子网掩码必须与此处子网掩码设置相同。

5.4.2 WAN口设置

选择菜单**网络参数→WAN口设置**，您可以在随后出现的界面中配置WAN口的网络参数。

1. WAN 是广域网(Wide Area Network)的缩写。在 WAN 设置中全部 IP 信息都是公有 IP 地址，可以在互联网上访问。该 WAN 口一共提供 7 种上网方式：动态 IP、静态 IP、PPPoE、IEEE802.1X+动态 IP、IEEE802.1X+静态 IP、PPTP、L2TP。具体配置时，请首先选择您所需要的 WAN 口连接类型，即您的上网方式，本路由器默认上网方式为动态 IP。

2. 动态 IP

选择**动态IP**，路由器将从ISP自动(网络服务提供商)获取IP地址。当ISP未给您提供任何IP网络参数时，请选择这种连接方式。如图2。

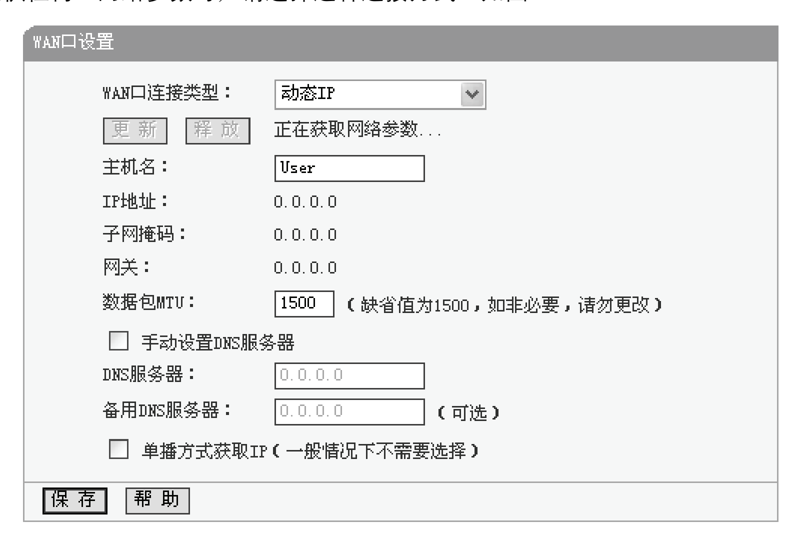


图 2 WAN 口设置-动态 IP

- 更新：单击**更新**按钮，路由器将从ISP的DHCP服务器动态得到IP地址、子网掩码、网关以及DNS服务器，并在界面中显示出来。
- 释放：单击**释放**按钮，路由器将发送DHCP释放请求给ISP的DHCP服务器，释放IP地址、子网掩码、网关以及DNS服务器设置。

- 数据包MTU：MTU全称为最大数据传输单元，缺省为1500。请向ISP咨询是否需要更改。如非特别需要，一般不要更改。
- DNS服务器、备用DNS服务器：该处显示从ISP处自动获得的DNS服务器地址。若选择**手动设置DNS服务器**，则您可以在此处手动设置DNS服务器和备用DNS服务器(至少设置一个)，连接时，路由器将优先使用手动设置的DNS服务器。
- 单播方式获取IP：由于少数ISP的DHCP服务器不支持广播的请求方式，所以当您在网络连接正常的情况下无法获取IP地址时，请选择该项。

完成更改后，点击**保存**按钮。

3. 静态 IP

当ISP给您提供了所有WAN IP信息时，请选择**静态IP**，并在下图3界面中输入IP地址、子网掩码、网关和DNS地址(一个或多个)。具体设置网络参数时，若不清楚，请咨询ISP。如图3。

WAN口设置

WAN口连接类型：	静态IP	
IP地址：	0.0.0.0	
子网掩码：	0.0.0.0	
网关：	0.0.0.0	（可选）
数据包MTU：	1500	（缺省值为1500，如非必要，请勿更改）
DNS服务器：	0.0.0.0	（可选）
备用DNS服务器：	0.0.0.0	（可选）

保 存　帮 助

图 3 WAN 口设置-静态 IP

- IP地址：本路由器对广域网的IP地址。请填入ISP提供的公共IP地址，必须设置。
- 子网掩码：本路由器对广域网的子网掩码。请填入ISP提供的子网掩码。根据不同的网络类型子网掩码不同，一般为255.255.255.0(C类)。
- 网关：请填入ISP提供给您的网关。它是连接的ISP的IP地址。

- 数据包MTU：MTU全称为数据传输单元，缺省为1500。请向ISP咨询是否需要更改。如非特别需要，一般不要更改。
- DNS服务器、备用DNS服务器：ISP一般至少会提供一个DNS(域名服务器)地址，若提供了两个DNS地址则将其中一个填入“备用DNS服务器”栏。

完成更改后，点击**保存**按钮。

4. PPPoE

如果ISP给您提供的是**PPPoE**(以太网上的点到点连接)，ISP会给您提供上网账号和上网口令。具体设置时，若不清楚，请咨询ISP。如图4。

WAN口设置

WAN口连接类型： PPPoE
上网账号： username
上网口令： ●●●●●●●●●●●●●●

如果正常拨号模式下无法连接成功，请依次尝试下列模式中的特殊拨号模式：

- ⦿ 正常拨号模式
- ○ 特殊拨号模式1
- ○ 特殊拨号模式2

根据您的需要，请选择对应的连接模式：

- ⦿ 按需连接，在有访问时自动连接
  自动断线等待时间：15 分 （0 表示不自动断线）
- ○ 自动连接，在开机和断线后自动连接
- ○ 定时连接，在指定的时间段自动连接
  注意：只有当您到“系统工具”菜单的“时间设置”项设置了当前时间后，“定时连接”功能才能生效。
  连接时段：从 0 时 0 分到 23 时 59 分
- ○ 手动连接，由用户手动连接
  自动断线等待时间：15 分 （0 表示不自动断线）

连 接　断 线

高级设置

保 存　帮 助

图 4 WAN 口设置-PPPoE

- 上网账号、上网口令：请正确填入ISP提供的上网账号和口令，必须填写。

- 按需连接：若选择**按需连接**模式，当有来自局域网的网络访问请求时，系统会自动进行连接。若在设定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。对于采用按使用时间进行交费的用户，可以选择该项连接方式，有效节省上网费用。
- 自动断线等待时间：如果自动断线等待时间T不等于0(默认时间为15分钟)，则在检测到连续T分钟内没有网络访问流量时自动断开网络连接，保护您的上网资源。此项设置仅对“按需连接”和“手动连接”生效。
- 自动连接：若选择**自动连接**模式，则在开机后系统自动进行连接。在使用过程中，如果由于外部原因，网络被断开，系统则会每隔一段时间(30秒)尝试连接，直到成功连接为止。若您的网络服务是包月交费形式，可以选择该项连接方式。
- 定时连接：若选择**定时连接**模式，则系统会在连接时段的开始时刻进行网络连接，在指定的终止时刻断开网络连接。选择此连接模式，可以有效控制内网用户的上网时间。
- 手动连接：选择该项，开机后需要用户手动才能进行拨号连接，若在指定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若您的网络服务是按使用时间进行交费，可以选择该项连接方式。
- 连接/断线：单击此按钮，可进行即时的连接/断线操作。

若需要进一步设置，可以点击**高级设置**按钮，在下图5界面中进行高级设置。

PPPoE高级设置

数据包MTU(字节)： 1480 (缺省值为1480，如非必要，请勿修改)

服务名： (如非必要，请勿填写)

服务器名： (如非必要，请勿填写)

☐ 使用ISP指定的IP地址

ISP指定的IP地址： 0.0.0.0

在线检测间隔时间： 0 秒 (0 ~ 120 秒, 0 表示不发送)

☐ 手动设置DNS服务器

DNS服务器： 0.0.0.0

备用DNS服务器： 0.0.0.0 (可选)

返 回

保 存 帮 助

图 5 WAN 口设置-PPPoE-高级设置

- 数据包MTU：填入网络数据包的MTU值，缺省为1480，如非特别需要，一般不要更改。
- 服务名、服务器名称：如果不是ISP特别要求，请不要填写这两项。
- 使用ISP指定IP地址：该项仅适用于静态PPPoE。如果您的ISP提供上网账号和口令时，亦提供了IP地址，请选中此选择框，并输入PPPoE连接的静态IP地址。
- 在线检测间隔时间：设置该值后，路由器将根据指定的时间间隔发送检测信号，以检测服务器是否在线。如果该值为0，则表示不发送检测信号。
- DNS服务器、备用DNS服务器：该处显示从ISP处自动获得的DNS服务器地址。若选择**手动设置DNS服务器**，则您可以在此处手动设置DNS服务器和备用DNS服务器(至少设置一个)，连接时，路由器将优先使用手动设置的DNS服务器。

完成更改后，点击**保存**按钮。

5. IEEE802.1X+动态 IP

如果ISP给您提供的是**IEEE802.1X+动态IP**上网方式，您可以自动从ISP获取IP地址，但是首先要通过IEEE802.1X认证，ISP会给您提供认证用户名和认证密码。具体设置时，若不清楚，请咨询ISP。如图6。

WAN口设置

WAN口连接类型： 802.1X + 动态IP

用户名： username

密码： ●●●●●●●●●●

登 录　退 出

IP地址： 0.0.0.0

子网掩码： 0.0.0.0

网关： 0.0.0.0

更 新　释 放

数据包MTU(字节)： 1500 （默认是1500，如非必要，请勿修改）

☐ 手动设置DNS服务器

DNS服务器： 0.0.0.0

备用DNS服务器： 0.0.0.0 （可选）

☐ 单播方式获取IP （一般情况下请勿选择）

保 存　帮 助

图 6 WAN 口设置-IEEE802.1X+动态 IP

- 用户名、密码：请正确填入ISP提供的认证用户名和密码，必须填写。
- 登录：当正确输入用户名和密码后，点击该按钮，可以登录服务器进行IEEE802.1X认证。
- 退出：当无上网需要时，可以点击该按钮，退出认证。
- 更新：当IEEE802.1X认证成功后(界面会显示“登录成功!”)，单击**更新**按钮，路由器将更新从ISP获取的WAN口IP地址、子网掩码、网关以及DNS服务器设置。
- 释放：单击**释放**按钮，路由器将发送DHCP释放请求给ISP的DHCP服务器，释放IP地址、子网掩码、网关以及DNS服务器设置。
- 数据包MTU(字节)：请填入网络数据包的MTU值，缺省为1500，如非特别需要，一般不要更改。

- DNS服务器、备用DNS服务器：该处显示从ISP处自动获得的DNS服务器地址。若选择**手动设置DNS服务器**，则您可以在此处手动设置DNS服务器和备用DNS服务器(至少设置一个)，连接时，路由器将优先使用手动设置的DNS服务器。
- 单播方式获取IP：由于少数ISP的DHCP服务器不支持广播的请求方式，所以当您在网络连接正常的情况下无法获取IP地址时，请选择该项。

完成更改后，点击**保存**按钮。

6. IEEE802.1X+静态 IP

如果ISP给您提供的是**IEEE802.1X+静态IP**上网方式，ISP会给您提供WAN口静态IP地址信息，但是首先要通过IEEE802.1X认证，ISP会给您提供认证用户名和认证密码。具体设置时，若不清楚，请咨询ISP。如图7。

WAN口设置

WAN口连接类型： 802.1X + 静态IP
用户名： username
密码： ●●●●●●●●●●
登 录 退 出
IP 地址： 0.0.0.0
子网掩码： 0.0.0.0
网关： 0.0.0.0 （可选）
数据包MTU(字节)： 1500 （默认是1500，如非必要，请勿修改）
DNS服务器： 0.0.0.0 （可选）
备用DNS服务器： 0.0.0.0 （可选）
保 存 帮 助

图 7 WAN 口设置-IEEE802.1X+静态 IP

- 用户名、密码：请正确填入ISP提供的认证用户名和密码，必须填写。
- 登录：当正确输入用户名和密码后，点击该按钮，可以登录服务器进行IEEE802.1X认证。
- 退出：当无上网需要时，可以点击该按钮，退出认证。
- IP地址：本路由器对广域网的IP地址。请填入ISP提供的静态IP地址，必须

设置。

- 子网掩码：本路由器对广域网的子网掩码。请填入ISP提供的子网掩码。根据不同的网络类型子网掩码不同，一般为255.255.255.0(C类)。
- 网关：请填入ISP提供给您的网关。
- 数据包MTU(字节)：请填入网络数据包的MTU值，缺省为1500，如非特别需要，一般不要更改。
- DNS服务器、备用DNS服务器：ISP一般至少会提供一个DNS(域名服务器)地址，若提供了两个DNS地址则将其中一个填入"备用DNS服务器"栏。

完成更改后，点击**保存**按钮。

7. L2TP

如果ISP给您提供的是**L2TP**上网方式，ISP会给您提供上网账号和上网口令。具体设置时，若不清楚，请咨询ISP。如图8。

WAN口设置

WAN口连接类型： L2TP

上网帐号： username
上网口令： ●●●●●●●●●
连 接 断 线 未连接

动态 IP 静态 IP
服务器 IP /域名：
IP 地址： 0.0.0.0
子网掩码： 0.0.0.0
网关： 0.0.0.0
DNS： 0.0.0.0 , 0.0.0.0

Internet IP： 0.0.0.0
Internet DNS： 0.0.0.0 , 0.0.0.0
数据包MTU(字节)： 1460 （缺省值为1460，如非必要，请勿修改）

根据您的需要，请选择对应的连接模式：
自动断线等待时间： 15 分 （0 表示不自动断线）
按需连接，在有访问数据时自动进行连接
自动连接，在开机和断线后自动连接
手动连接，由用户手动连接

保 存 帮 助

图 8 WAN 口设置-L2TP

- 上网帐号、上网口令：请正确填入ISP提供的帐号和口令，必须填写。
- 连接、断线：单击此按钮，可进行即时的连接或断线操作。
- 动态IP、静态IP：请根据实际情况选择IP类型(图8选择动态IP)。如果您可以自动从ISP获取IP地址，请选择**动态IP**；如果您拥有ISP提供的固定IP地址，请选择**静态IP**，并在随后的界面中设置WAN口静态IP信息(选择不同的IP类型，设置界面不同)。
- 服务器IP/域名：请正确填入ISP为您提供的IP地址或域名，此项必须填写。
- 数据包MTU(字节)：请填入网络数据包的MTU值，缺省为1460，如非特别需要，一般不要更改。

- 自动断线等待时间：如果自动断线等待时间T不等于0(默认时间为15分钟)，则在检测到连续T分钟内没有网络访问请求时，系统会自动断开网络连接，保护您的上网资源。此项设置仅对“按需连接”和“手动连接”生效。
- 按需连接：若选择按需连接模式，当有来自局域网的网络访问请求时，系统会自动进行连接。若在设定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。对于采用按使用时间进行交费的用户，可以选择该项连接方式，有效节省上网费用。
- 自动连接：若选择自动连接模式，则在开机后系统自动进行连接。在使用过程中，如果由于外部原因，网络被断开，系统则会每隔一段时间(30秒)尝试连接，直到成功连接为止。若您的网络服务是包月交费形式，可以选择该项连接方式。
- 手动连接：选择该项，开机后需要用户手动才能进行拨号连接，若在指定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若您的网络服务是按使用时间进行交费，可以选择该项连接方式。

完成更改后，点击**保存**按钮。

8. PPTP

如果您选择的是**PPTP**上网方式，ISP会给您提供上网账号和上网口令。具体设置时，若不清楚，请咨询ISP。如图9。

WAN口设置

WAN口连接类型： PPTP

上网帐号： username

上网口令： ●●●●●●●●●●

连 接　断 线　未连接

○ 动态 IP　◉ 静态 IP

服务器 IP /域名：

IP 地址： 0.0.0.0

子网掩码： 0.0.0.0

网关： 0.0.0.0

DNS： 0.0.0.0

Internet IP： 0.0.0.0

Internet DNS： 0.0.0.0 , 0.0.0.0

数据包MTU(字节)： 1420 （缺省值为1420，如非必要，请勿修改）

根据您的需要，请选择对应的连接模式：

自动断线等待时间： 15 分 （0 表示不自动断线）

◉ 按需连接，在有访问数据时自动进行连接

○ 自动连接，在开机和断线后自动连接

○ 手动连接，由用户手动连接

保 存　帮 助

图 9 WAN 口设置-PPTP

- 上网帐号、上网口令：请正确填入ISP提供的帐号和口令，必须填写。
- 连接、断线：单击此按钮，可进行即时的连接或断线操作。
- 动态IP、静态IP：请根据实际情况选择IP类型(图9选择静态IP)。如果您可以自动从ISP获取IP地址，请选择**动态IP**；如果您拥有ISP提供的固定IP地址，请选择**静态IP**，并在随后的界面中设置WAN口静态IP信息(选择不同的IP类型，设置界面不同)。
- 服务器IP/域名：请正确填入ISP为您提供的IP地址或域名，此项必须填写。
- 数据包MTU(字节)：请填入网络数据包的MTU值，缺省为1420，如非特别

需要，一般不要更改。

- 自动断线等待时间：如果自动断线等待时间T不等于0(默认时间为15分钟)，则在检测到连续T分钟内没有网络访问请求时，系统会自动断开网络连接，保护您的上网资源。此项设置仅对“按需连接”和“手动连接”生效。
- 按需连接：若选择按需连接模式，当有来自局域网的网络访问请求时，系统会自动进行连接。若在设定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。对于采用按使用时间进行交费的用户，可以选择该项连接方式，有效节省上网费用。
- 自动连接：若选择自动连接模式，则在开机后系统自动进行连接。在使用过程中，如果由于外部原因，网络被断开，系统则会每隔一段时间(30秒)尝试连接，直到成功连接为止。若您的网络服务是包月交费形式，可以选择该项连接方式。
- 手动连接：选择该项，开机后需要用户手动才能进行拨号连接，若在指定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若您的网络服务是按使用时间进行交费，可以选择该项连接方式。

完成更改后，点击**保存**按钮。

5.4.3 MAC地址克隆

选择菜单**网络参数→MAC地址克隆**，您可以在下图10界面中设置路由器对广域网的MAC地址。

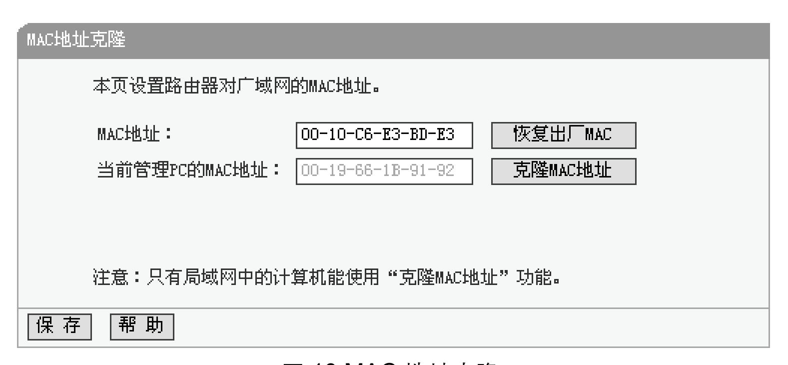


图 10 MAC 地址克隆

- MAC地址：此项为路由器对广域网的MAC地址，默认的MAC地址为路由器上WAN的物理接口MAC地址。某些ISP可能会要求对MAC地址进行绑定，此时ISP会提供一个有效的MAC地址给用户，您只要根据它所提供的值，输入到“**MAC地址**”栏。不建议更改MAC地址，除非ISP有特别要求。
- 当前管理PC的MAC地址：该处显示当前正在管理路由器的计算机的MAC地址。
- 恢复出厂MAC：单击此按钮，即可恢复MAC地址为出厂时的默认值。
- 克隆MAC地址：单击此按钮，可将当前管理PC的MAC地址克隆到“MAC地址”栏内。若您的ISP提供服务时要求进行MAC地址克隆，则可进行该项操作，否则不要克隆MAC地址。

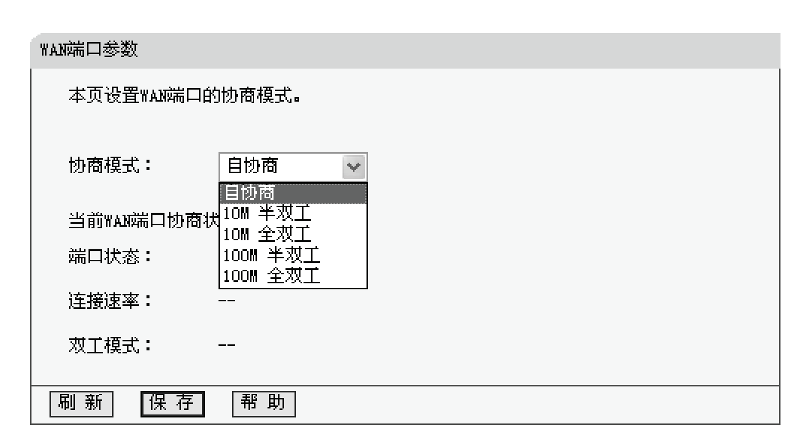
完成更改后，点击**保存**按钮，路由器会自动重启。

⚠ 注意：

只有局域网中的计算机才能使用“克隆MAC地址”功能。

5.4.4 WAN端口参数

选择网络参数下的 WAN 端口参数，您将进入下面的设置界面。该页面提供 WAN 端口的协商模式设置，并显示端口状态和连接速率等信息。



- **协商模式**：您可以根据需要选择协商模式：自协商、10M半双工、10M全双工、100M半双工或100M全双工模式。

➢ **端口状态**：显示端口连接状态，即是否已经连接上。

➢ **连接速率**：显示端口连接采用的速率。

➢ **双工模式**：显示端口通信采用的双工模式，全双工或半双工。

⚠ 注意：

WAN端口的速率/双工模式在默认情况下是“自协商”模式，修改该选项会影响链路的性能，如非必要，请勿更改。

5.5DHCP 服务器

选择菜单**DHCP服务器**，您可以看到：

- DHCP服务器
  - DHCP服务
  - 客户端列表
  - 静态地址分配

单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.5.1 DHCP服务

选择菜单**DHCP服务器→DHCP服务**，您将看到DHCP设置界面，如下图所示。

DHCP指动态主机控制协议(Dynamic Host Control Protocol)。FR516/FR524有一个内置的DHCP服务器，它能够自动分配IP地址给局域网中的计算机。对用户来说，为局域网中的所有计算机配置TCP/IP协议参数并不是一件容易的事，它包括IP地址、子网掩码、网关、以及DNS服务器的设置等。若使用DHCP服务则可以解决这些问题。您可以按照下面各子项说明正确设置这些参数。

DHCP服务

本路由器内建DHCP服务器，它能自动替您配置局域网中各计算机的TCP/IP协议。

DHCP服务器：	○不启用 ◉启用
地址池开始地址：	192.168.1.100
地址池结束地址：	192.168.1.199
地址租期：	120 分钟（1~2880分钟，缺省为120分钟）
网关：	0.0.0.0 （可选）
缺省域名：	（可选）
主DNS服务器：	0.0.0.0 （可选）
备用DNS服务器：	0.0.0.0 （可选）

保 存 帮 助

图 11 DHCP 服务

- 地址池开始地址、地址池结束地址: 这两项为DHCP服务器自动分配IP地址时的起始地址和结束地址。设置这两项后，内网主机得到的IP地址将介于这两个地址之间。
- 地址租期: 该项指DHCP服务器给客户端主机分配的动态IP地址的有效使用时间。在该段时间内，服务器不会将该IP地址分配给其它主机。
- 网关: 此项应填入路由器LAN口的IP地址，缺省是192.168.1.1。
- 缺省域名: 此项为可选项，应填入本地网域名(默认为空)。
- 主DNS服务器、备用DNS服务器: 这两项为可选项，可以填入ISP提供给您的DNS服务器，不清楚可以向ISP询问。

完成更改后，点击**保存**按钮。

⚠ *注意:*

若要使用本路由器的DHCP服务器功能，局域网中计算机的TCP/IP协议项必须设置为“自动获得IP地址”。此功能需要重启路由器后才生效。

5.5.2 客户端列表

选择菜单**DHCP服务器→客户端列表**, 您可以查看所有通过DHCP服务器获得IP地址的主机的信息，单击**刷新**按钮可以更新表中信息，如图12。

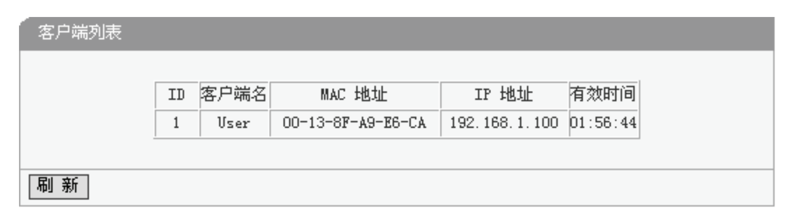


图 12 客户端列表

- 客户端名：该处显示获得了IP地址的客户端计算机的名称。
- MAC地址：该处显示获得了IP地址的客户端计算机的MAC地址。
- IP地址：该处显示DHCP服务器分配给客户端主机的IP地址。
- 有效时间：该项指客户端主机获得的IP地址离到期的时间，每个IP地址都有一定的租用时间，客户端软件会在租期到期前自动续约。

5.5.3 静态地址分配

选择菜单**DHCP服务器→静态地址分配**，您可以在下图13界面中设置静态IP地址。

静态地址分配功能可以为指定MAC地址的计算机预留静态IP地址。当该计算机请求DHCP服务器分配IP地址时，DHCP服务器将给它分配表中预留的IP地址。并且一旦采用，该主机的IP地址将不再改变。

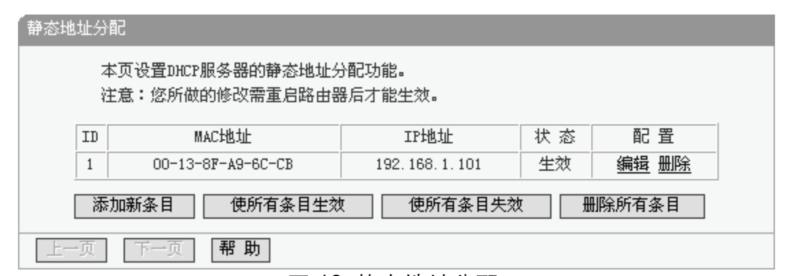


图 13 静态地址分配

- MAC地址：该项指定将要预留静态IP地址的计算机的MAC地址。
- IP地址：该项指定给内网主机预留的IP地址。
- 状态：显示该条目状态“生效”或“失效”，只有状态为生效时，本条过滤规则才生效。

- 添加新条目：单击该按钮，你可以在随后的界面中添加新的静态地址条目，如图14。
- 使所有条目生效：单击该按钮，您可以使表中的所有条目生效。
- 使所有条目失效：单击该按钮，您可以使表中的所有条目失效。
- 删除所有条目：单击该按钮，您可以删除表中所有的条目。

例1：如果您希望给局域网中MAC地址为00-13-8F-A9-6C-CB的计算机预留IP地址：192.168.1.101。这时您可以按照如下步骤设置：

第一步：在图13界面中单击**添加新条目**。

第二步：在图14界面中设置**MAC地址**为00-13-8F-A9-6C-CB，**IP地址**为192.168.1.101，**状态**为生效。

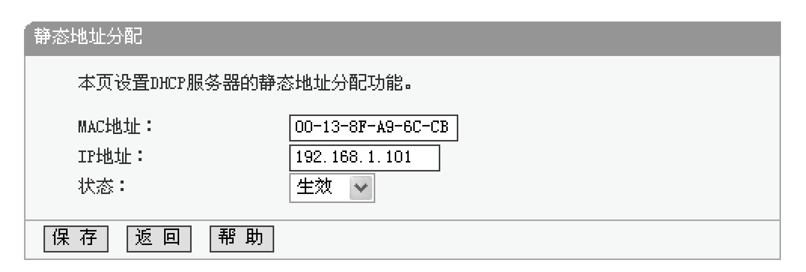


图 14 添加静态地址条目

第三步：点击**保存**按钮。



此功能需要重启路由器后才能生效。

5.6 转发规则

选择菜单**转发规则**，您可以看到：

- 转发规则
  - 虚拟服务器
  - 特殊应用程序
  - DMZ主机
  - UPnP设置

单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.6.1 虚拟服务器

选择菜单**转发规则→虚拟服务器**，您可以在下图15界面中设置虚拟服务器条目。

FR516/FR524可配置为虚拟服务器，它能使通过公共IP地址访问Web或FTP等服务的远程用户自动转向到局域网中的本地服务器。

FR516/FR524内置的防火墙特性能过滤掉未被识别的包，保护您的局域网络。在路由器默认设置下，局域网中所有的计算机都不能被外界看到。如果希望在保护局域网内部不被侵袭的前提下，某些LAN中的计算机在广域网上可见，请使用虚拟服务器。

虚拟服务器可以定义一个服务端口，外网所有对此端口的服务请求都将改发给路由器指定的局域网中的服务器(通过IP地址指定)，这样外网的用户便能成功访问局域网中的服务器，而不影响局域网内部的网络安全。


虚拟服务器

虚拟服务器定义了广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过IP地址指定的局域网网络服务器。

ID	服务端口	IP地址	协议	状态	配置
1	21	192.168.1.100	TCP	生效	编辑 删除
2	80	192.168.1.101	ALL	生效	编辑 删除

添加新条目 使所有条目生效 使所有条目失效 删除所有条目

上一页 下一页 帮 助

图 15 虚拟服务器

- 服务端口：此项为路由器提供给广域网的服务端口，广域网用户通过向该端口发送请求来获取服务。可输入单个端口值或端口段。端口段输入格式为“开始端口-结束端口”，中间用“-”隔开。
- IP地址：局域网中被指定提供虚拟服务的服务器地址。
- 协议：虚拟服务所用的协议，可供选择的有：TCP、UDP和ALL。若对采用的协议不清楚，可以选择ALL。
- 状态：该项显示该条目状态“生效”或“失效”，只有状态为生效时，本条目的

设置才生效。

例1：如果希望广域网用户通过端口21访问您的FTP服务器，FTP服务器在局域网中的IP地址为192.168.1.100，协议选择为TCP，则您可以按照如下步骤设置：

第一步：在图15界面中点击**添加新条目**按钮。

第二步：在图16界面中点击“常用服务端口”下拉菜单，查找FTP服务，选中“FTP”服务。

虚拟服务器

虚拟服务器定义了广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过IP地址指定的局域网网络服务器。

服务端口号：	21	(XX-XX or XX)
IP地址：	192.168.1.100	
协议：	TCP	
状态：	生效	
常用服务端口号：	FTP	

保 存　返 回　帮 助

图 16 添加虚拟服务条目

- 常用服务端口：在“常用服务端口”中，列出了常用协议的端口，您可以直接从其中选择一个，然后选择需要添加到表中的ID序列号，最后单击**填空到**按钮，系统则会将该服务的端口号、协议类型，自动添加到对应序列的“服务端口号”和“协议”项中，您只需要再为其指定服务器IP地址并启用即可。对于常用服务端口中没有列出的端口，如果需要，也可以在服务端口处手动添加。

第三步：输入IP地址为“192.168.1.100”，设置条目状态为“生效”。

第四步：单击**保存**按钮。

设置好以后，您只要在局域网的服务器上进行相应的设置，广域网的计算机就可以访问到您局域网的服务器上了。

例2：如果希望广域网用户通过端口80访问您的Web服务器，Web服务器在局域网中的IP地址为192.168.1.101，协议选择为ALL，则您可以按照如下步骤设置：

第一步：在图15界面中点击**添加新条目**按钮。

第二步：在图16界面中设置服务端口为“80”，输入IP地址为“192.168.1.101”，选择协议为“ALL”。

第三步：点击**保存**按钮。

例1和例2设置完成后生成的虚拟服务列表为：

ID	服务端口	IP地址	协议	状态	配置
1	21	192.168.1.100	TCP	生效	编辑 删除
2	80	192.168.1.101	ALL	生效	编辑 删除

注意：

1) 如果设置了服务端口为80的虚拟服务器，则需要将安全设置→远端WEB管理的“WEB管理端口”设置为80以外的值，如88，否则会发生冲突，从而导致虚拟服务器不起作用。

2) 例1中的服务在“常用服务端口”中已经提供，对于“常用服务端口”中没有提供的服务，可参照例2来添加。

5.6.2 特殊应用程序

选择菜单**转发规则→特殊应用程序**，您可以在下图17界面中设置特殊应用程序条目。

某些应用需要多条连接，如Internet网络游戏、视频会议、网络电话等。由于防火墙的存在，这些程序无法在简单的NAT路由器下工作。然而，特殊应用程序使得某些这样的应用程序能够在NAT路由器下工作。当一个应用程序向触发端口上发起连接时，对应的所有开放端口将会打开，以备后续连接并提供服务。


特殊应用程序

某些程序需要多条连接，如Internet游戏，视频会议，网络电话等。由于防火墙的存在，这些程序无法在简单的NAT 路由下工作。特殊应用程序使得某些这样的应用程序能够在NAT路由下工作。

ID	触发端口	触发协议	开放端口	开放协议	状态	配置
1	7175	ALL	51200-51201,51210	ALL	生效	编辑 删除
2	6112	ALL	6112	ALL	生效	编辑 删除

添加新条目 使所有条目生效 使所有条目失效 删除所有条目

上一页 下一页 帮 助

图 17 特殊应用程序

- 触发端口：该端口是应用程序首先发起连接的端口，只有在该端口上发起连接，开放端口中的所有端口才可以开放，否则开放端口是不会开放的。
- 触发协议：代表触发端口上使用的协议，可以选择ALL、UDP或TCP。若不清楚采用哪种协议，可以选用ALL。
- 开放端口：当向触发端口上成功发起连接后，对应的开放端口会打开，应用程序便可以向该开放端口发起后续的连接。此处可以输入一个或者多个端口或端口段，端口段输入格式为“开始端口-结束端口”，中间用“-”隔开，不同的端口段用“,”隔开。
- 开放协议：代表开放端口上使用的协议，可以选择ALL、UDP和TCP。若不清楚采用哪种协议，可以选用ALL。
- 状态：该项显示该条目状态“生效”或“失效”，只有状态为生效时，本条目的设置才生效。

在图17界面中点击**添加新条目**按钮，您可以在下图18界面中添加新的特殊应用程序条目。

特殊应用程序

某些程序需要多条连接，如Internet游戏，视频会议，网络电话等。由于防火墙的存在，这些程序无法在简单的NAT 路由下工作。特殊应用程序使得某些这样的应用程序能够在NAT路由下工作。

触发端口：	7175
触发协议：	ALL
开放端口：	51200-51201,51210
开放协议：	ALL
状态：	生效
常用应用程序：	Dialpad

保 存　返 回　帮 助

图 18 添加特殊应用程序条目

- 常用应用程序：在"常用应用程序"中，列出了常用的应用程序，您可以直接从中选择一个，然后选择需要添加到表中的ID序列号，最后单击填空到按钮，系统则会自动将该常用应用程序的触发端口号和开放端口号添加到对应的"触发端口"和"开放端口"项中，并且会启用该条目。对于常用应用程序中没有列出的程序，您可以手动添加。

完成设置后，点击**保存**按钮。

5.6.3 DMZ主机

选择菜单**转发规则→DMZ主机**，您可以在下图19界面中设置DMZ(非军事区)主机。

局域网中设置DMZ主机后，该主机将完全暴露给广域网，可以实现双向无限制通信。具体设置时，只需输入局域网中指定为DMZ主机的IP地址，然后选中启用并点击**保存**即可。向DMZ添加客户机可能会给本地网络带来不安全因素，因此不要轻易使用这一选项。

DMZ主机

在某些特殊情况下，需要让局域网中的一台计算机完全暴露给广域网，以实现双向通信，此时可以把该计算机设置为DMZ主机。
（注意：设置DMZ主机之后，与该IP相关的防火墙设置将不起作用。）

DMZ 状态： ◉启用 ○不启用

DMZ 主机IP地址： 192.168.1.102

保 存 帮 助

图 19 DMZ 主机

5.6.4 UPnP设置

选择菜单**转发规则→UPnP设置**，您可以在下图20界面中查看UPnP信息。

依靠UPnP(Universal Plug and Play)协议，局域网中的主机可以请求路由器进行特定的端口转换，使得外部主机能够在需要时访问内部主机上的资源，例如，Windows XP和Windows ME系统上安装的MSN Messenger，在使用音频和视频通话时就可以利用UPnP协议，这样原本受限于NAT的功能便可以恢复正常使用。

UPnP设置

本页设置/显示UPnP的设置以及工作状态。

当前UPnP状态： **已开启** 关闭UPnP

当前UPnP设置列表

ID	应用描述	外部端口	协议类型	内部端口	IP地址	状态
1	ftp	21	TCP	21	192.168.1.100	已启用

刷 新

图 20 UPnP 设置

- 应用描述：应用程序通过UPnP向路由器请求端口转换时给出的描述。
- 外部端口：端口转换使用的路由器端口号。
- 协议类型：表明是对TCP还是UDP进行端口转换。
- 内部端口：需要进行端口转换的主机端口号。
- IP地址：需要进行端口转换的主机IP地址。
- 状态：该项显示条目是否已经启用。
- 刷新：单击该按钮，可以刷新当前的UPnP列表信息。

UPnP的使用方法如下:

1. 点击**启用 UPnP** 按钮开启 UPnP 功能。

2. 当 MSN Messenger 等程序在运行中使用本功能时，按**刷新**按钮可以看到端口转换信息。端口转换信息由应用程序发出请求时提供。

3. 如果需要将某条目手工删除，请在删除栏选中该条目，再点击右侧的**删除**按钮，此时被选中的条目将被删除；如果希望将表中所有条目删除，请点击**删除所有**按钮，并确认即可。

4. 不使用时请点击关闭 **UPnP** 按钮关闭 UPnP 功能。

注意:

1) 因为现阶段版本的UPnP协议的安全性还未得充分保证，在不需要时请关闭UPnP功能。

2) 只有支持UPnP协议的应用程序才能使用本功能，MSN Messenger还可能需要操作系统的支持(如Windows XP/ME)。

3) UPnP功能需要操作系统的支持(如Windows XP/ME)。

5.7 安全设置

选择菜单**安全设置**，您可以看到:

- 安全设置
  - 防火墙设置
  - IP地址过滤
  - 域名过滤
  - MAC地址过滤
  - 远端WEB管理
  - 高级安全设置

单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.7.1 防火墙设置

选择菜单**安全设置→防火墙设置**，您可以在下图21界面中设置路由器的安全项。

该界面控制路由器防火墙总功能的开启，以及各子项功能：IP地址过滤、域名过滤和MAC地址过滤功能的开启和过滤规则。只有防火墙的总开关开启后，后续的安全设置才能够生效，反之，则不能生效。(建议在过滤规则设置完成后再开启防火墙总开关)



图 21 防火墙设置

- 开启防火墙：这是防火墙的总开关，只有该项开启后，IP地址过滤、域名过滤、MAC地址过滤功能才能启用，反之，则不能被启用。
- 开启IP地址过滤: 关闭或开启IP地址过滤功能并选择缺省过滤规则。只有“开启防火墙”启用后，该项才能生效。
- 开启域名过滤：关闭或开启域名过滤功能。只有“开启防火墙”启用后，该项才能生效。
- 开启MAC地址过滤：关闭或开启MAC地址过滤功能并选择缺省过滤规则。

只有“开启防火墙”启用后，该项才能生效。

完成设置后，点击**保存**按钮。

5.7.2 IP地址过滤

选择菜单**安全设置→IP地址过滤**，您可以在下图22界面中查看并添加IP地址过滤条目。

使用IP地址过滤可以拒绝或允许局域网中计算机与互联网之间的通信。可以拒绝或允许特定IP地址的特定的端口号或所有端口号。

您可以利用按钮**添加新条目**来增加新的过滤规则，或者通过“修改”、“删除”链接来修改或删除已设过滤规则，甚至可以通过按钮**移动**来调整各条过滤规则的顺序，以达到不同的过滤优先级(ID序号越靠前则优先级越高)。

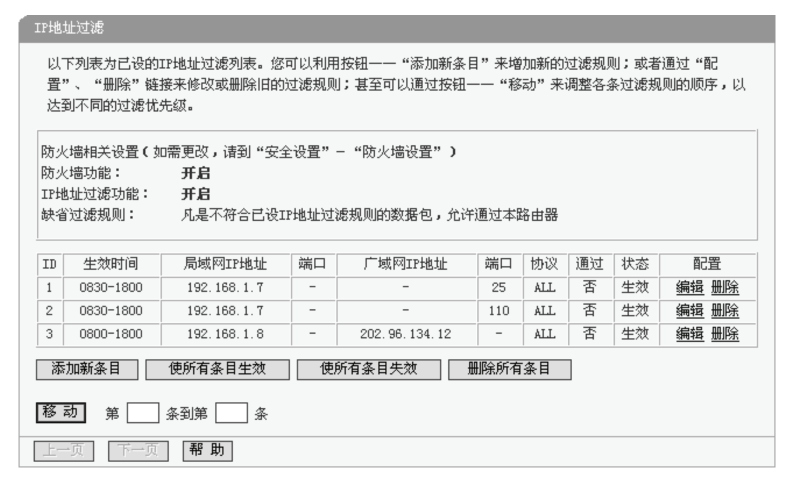


图 22 IP 地址过滤

- 生效时间：该项用来指定过滤条目的有效时间，在该段时间外，此过滤条目不起作用。
- 局域网IP地址：局域网中被控制的计算机的IP地址，为空表示对局域网中所有计算机进行控制。此处可以输入一个IP地址段，例如：192.168.1.123 – 192.168.1.185。
- (局域网)端口：局域网中被控制的计算机的服务端口，为空表示对该计算机

的所有服务端口进行控制。此处可以输入一个端口段，例如：1030－2000。

- 广域网IP地址：广域网中被控制的计算机(如网站服务器)的IP地址，为空表示对整个广域网进行控制。此处可以输入一个IP地址段，例如：61.145.238.6-61.145.238.47。
- (广域网)端口：广域网中被控制的计算机(如网站服务器)的服务端口，为空表示对该网站所有服务端口进行控制。此处可以输入一个端口段，例如：25-110。
- 协议：此处显示被控制的数据包所使用的协议。
- 通过：该项显示符合本条目所设置的规则的数据包是否可以通过路由器，"是"表示允许该条目通过路由器，"否"表示不允许该条目通过路由器。
- 状态：显示该条目状态"生效"或"失效"，只有状态为生效时，本条过滤规则才生效。

例1： 如果您希望禁止局域网中IP地址为192.168.1.7的计算机在8：30到18：00之间收发邮件，禁止IP地址为192.168.1.8的计算机在8：00到18：00之间访问IP为202.96.134.12的网站，对局域网中的其它计算机则不做任何限制，这时您可以按照如下步骤设置：

第一步：在图21界面中打开防火墙总开关。

第二步：在图21中开启"IP地址过滤"，设置"缺省过滤规则"为"凡是不符合已设IP地址过滤规则的数据包，允许通过本路由器"。

第三步：在图22界面中点击**添加新条目**，然后在下图23中按要求添加过滤条目。下图是禁止192.168.1.7的计算机在8：30到18：00之间发送邮件的设置，设置完成后，点击保存按钮。

IP地址过滤

本页添加新的、或者修改旧的IP地址过滤规则。

生效时间： 0830 - 1800
局域网IP地址： 192.168.1.7 -
局域网端口： -
广域网IP地址： -
广域网端口： 25 -
协 议: ALL
通 过： 禁止通过
状 态： 生效

保 存 返 回 帮 助

图 23 添加 IP 地址过滤条目

第四步：回到第三步，继续设置过滤条目：禁止局域网中IP地址为192.168.1.7的计算机在8：30到18：00之间接收邮件，禁止IP地址为192.168.1.8的计算机在8: 00到18: 00之间访问IP为202.96.134.12的网站。完成例1中设置一共需要设置3条IP过滤规则，依次对应下面列表中的三条过滤条目。

ID	生效时间	局域网IP地址	端口	广域网IP地址	端口	协议	通过	状态	配置
1	0830-1800	192.168.1.7	-	-	25	ALL	否	生效	编辑 删除
2	0830-1800	192.168.1.7	-	-	110	ALL	否	生效	编辑 删除
3	0800-1800	192.168.1.8	-	202.96.134.12	-	ALL	否	生效	编辑 删除

5.7.3 域名过滤

选择菜单**安全设置→域名过滤**，您可以在下图24界面中查看并添加域名过滤条目。

域名过滤可以阻止LAN中所有计算机访问广域网(如互联网)上的特定域名，该特性会拒绝所有到特定域名如http和ftp的请求。您可以利用按钮**添加新条目**来增加新的过滤规则，或者通过“修改”、“删除”链接来修改或删除旧的过滤规则。



域名过滤

本页通过域名过滤来限制局域网中的计算机对某些网站的访问。

防火墙相关设置（如需更改，请到“安全设置” - “防火墙设置”）
防火墙功能：　开启
域名过滤功能：　开启

ID	生效时间	域 名	状 态	配 置
1	0830-1800	www.yaohoo.com.cn	生效	编辑 删除
2	0830-1800	sina.com	生效	编辑 删除
3	0800-1200	.net	生效	编辑 删除

添加新条目　使所有条目生效　使所有条目失效　删除所有条目

上一页　下一页　帮 助

图 24 域名过滤

- 域名：拒绝被LAN计算机访问的域名。
- 状态：显示该条目状态“生效”或“失效”，只有状态为生效时，本条过滤规则才生效。

例 1：如果您希望禁止局域网中的计算机在8：30到18：00之间访问“www.yahoo.com.cn”、“sina.com”的网站，禁止局域网中的计算机在8：00到12：00之间访问所有以“.net”结尾的网站，这时您可以按照如下步骤设置：

第一步：在图21界面中打开防火墙总开关并开启“域名过滤”。

第二步: 在图24界面中点击**添加新条目**, 然后在下图25界面中设置条目信息。下图是在8：30到18：00之间拒绝访问www.yahoo.com.cn网站的设置，设置完成后，点击保存按钮。

域名过滤

本页通过域名过滤来限制局域网中的计算机对某些网站的访问。

生效时间　0830 - 1800
域 名:　www.yaohoo.com.cn
状 态:　生效

保 存　返 回　帮 助

图 25 添加域名过滤条目

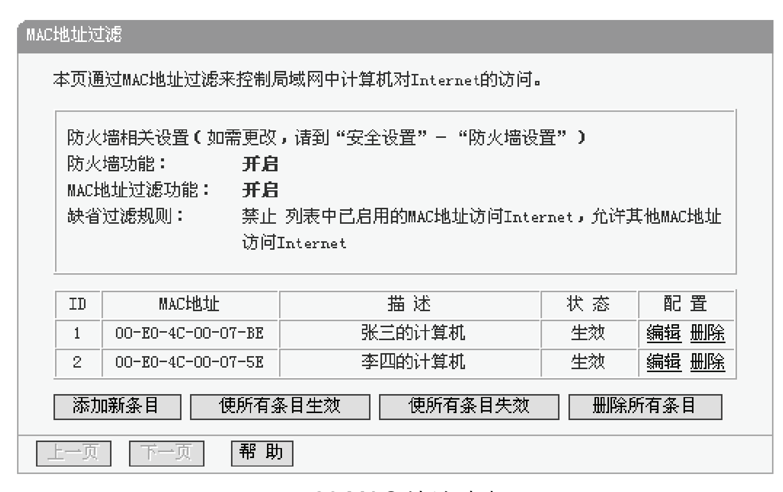
第三步：回到第二步，继续设置过滤条目：禁止局域网中的计算机在8：30到18：00之间访问“sina.com”，禁止局域网中的计算机在8：00到12：00之间访问所有以“.net”结尾的网站。完成例1中设置一共需要设置3条域名过滤规则，依次对应下面列表中的三条过滤条目。

ID	生效时间	域 名	状 态	配 置
1	0830-1800	www.yaohoo.com.cn	生效	编辑 删除
2	0830-1800	sina.com	生效	编辑 删除
3	0800-1200	.net	生效	编辑 删除

5.7.4 MAC地址过滤

选择菜单**安全设置→MAC地址过滤**，您可以在下图26界面中查看并添加MAC地址过滤条目。

MAC地址过滤功能通过MAC地址允许或拒绝局域网中计算机访问广域网，有效控制局域网内用户的上网权限。您可以利用按钮**添加新条目**来增加新的过滤规则；或者通过“修改”、“删除”链接来修改或删除旧的过滤规则。


MAC地址过滤

本页通过MAC地址过滤来控制局域网中计算机对Internet的访问。

防火墙相关设置（如需更改，请到“安全设置”－“防火墙设置”）
防火墙功能： **开启**
MAC地址过滤功能： **开启**
缺省过滤规则： 禁止 列表中已启用的MAC地址访问Internet，允许其他MAC地址访问Internet

ID	MAC地址	描 述	状 态	配 置
1	00-E0-4C-00-07-BE	张三的计算机	生效	编辑 删除
2	00-E0-4C-00-07-5E	李四的计算机	生效	编辑 删除

添加新条目 使所有条目生效 使所有条目失效 删除所有条目

上一页 下一页 帮 助

图 26 MAC 地址过滤

- MAC地址：该项是您希望管理的计算机的MAC地址。
- 描述：该项是对该计算机的适当描述。
- 状态：显示该条目状态“生效”或“失效”，只有状态为生效时，本条过滤规则

才生效。

例 1： 如果您不希望局域网中MAC地址为00-E0-4C-00-07-BE和00-E0-4C-00-07-5E的计算机访问Internet，而希望局域网中的其它计算机能访问Internet，这时您可以按照如下步骤设置MAC地址过滤表:

第一步：在图21界面中打开防火墙总开关。

第二步：在图21防火墙设置界面中开启“MAC地址过滤”，设置“缺省过滤规则”为“禁止已设MAC地址列表中已启用的MAC地址访问Internet，允许其它MAC地址访问Internet”。

第三步：在图26界面中点击**添加新条目**，然后在下图27界面中设置条目信息。下图是禁止MAC地址为00-E0-4C-00-07-BE的计算机访问Internet的设置，设置完成后，点击**保存**按钮。

MAC地址过滤

本页通过MAC地址过滤来控制局域网中计算机对Internet的访问。

MAC 地址： 00-E0-4C-00-07-BE

描 述： 张三的计算机

状 态： 生效

保 存 返 回 帮 助

图 27 添加 MAC 地址过滤条目

第四步：回到第三步，继续设置过滤条目：禁止MAC地址为00-E0-4C-00-07-5E的计算机访问Internet。完成例1中设置一共需要设置2条域名过滤规则，依次对应如下列表中的2条过滤条目。

ID	MAC地址	描 述	状 态	配 置
1	00-E0-4C-00-07-BE	张三的计算机	生效	编辑 删除
2	00-E0-4C-00-07-5E	李四的计算机	生效	编辑 删除

5.7.5 远端WEB管理

选择菜单**安全设置→远端WEB管理**。远端WEB管理功能可以允许用户通过Web浏览器从广域网配置路由器。本特性允许您从远程主机执行管理任务。您可以在下图28界面中设置管理IP地址和端口。

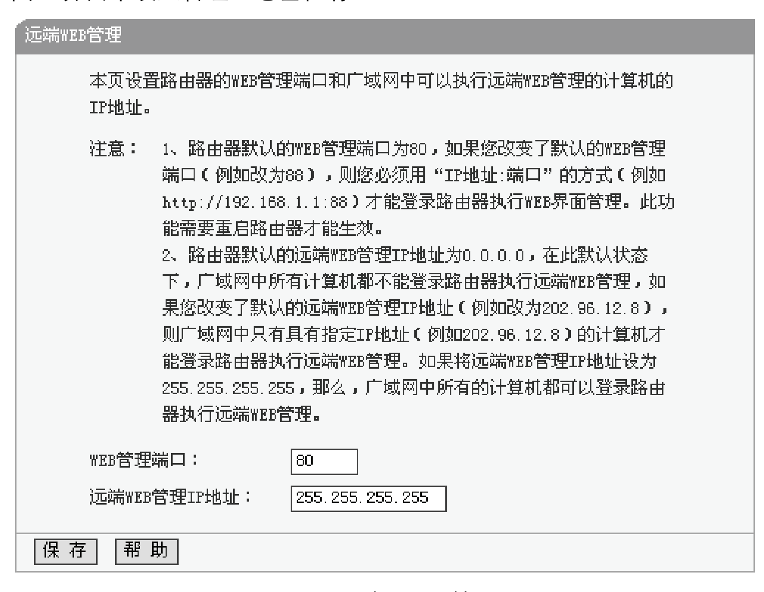


图 28 远端 WEB 管理

- WEB管理端口：用于访问宽带路由器的WEB管理端口号。
- 远端WEB管理IP地址：广域网中可以访问该路由器执行远端WEB管理的计算机IP地址。

完成更改后，点击**保存**按钮。

注意：

1) 路由器默认的WEB管理端口为80，如果您改变了默认的WEB管理端口(例如改为88)，则您必须用“IP地址:端口”的方式(例如http://192.168.1.1:88)才能登录路由器执行WEB界面管理。此功能需要重启路由器后才生效。

2) 路由器默认的远端WEB管理IP地址为0.0.0.0，在此默认状态下，广域网中所有计算机都不能登录路由器执行远端WEB管理，如果您改变了默认的远端WEB管理IP地址(则广域网中只有具有该指定IP地址的计算机才能登录路由器执行远端WEB管理。如果改为255.255.255.255，则WAN中所有主机都可以登录路由器执行远端WEB管理。

例1：如果您希望广域网中IP地址为202.96.134.13的计算机能够访问宽带路由器，执行远端WEB管理功能，WEB管理端口为80。则您可以进行如下设置：

第一步：设置WEB管理端口为“80”。

第二步：设置远端WEB管理IP地址为“255.255.255.255”或“202.96.134.13”。

这样，该计算机访问路由器管理界面时应该输入路由器WAN口的IP地址即可。

5.7.6 高级安全设置

选择菜单**安全设置→高级安全设置**，您可以在下图29界面中开启DoS(拒绝服务)攻击防范。完成更改后，点击**保存**按钮。

DoS攻击的目的是用极大量的虚拟信息流耗尽目标主机的资源，受害者被迫全力处理虚假信息流，从而影响对正常信息流的处理。如果DoS攻击始发自多个源地址，则称为分布式拒绝服务(DDoS) 攻击。通常DoS与DDoS攻击中的源地址都是欺骗性的。

高级安全选项

本页设置高级安全防范配置。只有当“DOS攻击防范”启用的时候，其后面的设置才能够生效。（注意：这里的“数据包统计时间间隔”与“系统工具”－“流量统计”中的“数据包统计时间间隔”为同一值，无论在哪一个模块进行修改都会覆盖另一模块里的数值。）
另外：由于“DoS攻击防范”的部分功能是以相关数据包的统计为依据的，因此，如果“系统工具”－“流量统计”中的流量统计功能被关闭，那么将会导致这部分功能失效。同时该功能还受“防火墙设置”中的“开启防火墙”的影响。

数据包统计时间间隔：（5～60） 10 秒

DoS攻击防范： ○不启用 ◉启用

开启ICMP-FLOOD攻击过滤： ☑

ICMP-FLOOD数据包阀值：（5～3600） 50 包/秒

开启UDP-FLOOD过滤： ☑

UDP-FLOOD数据包阀值：（5～3600） 500 包/秒

开启TCP-SYN-FLOOD攻击过滤： ☑

TCP-SYN-FLOOD数据包阀值：（5～3600） 50 包/秒

忽略来自WAN口的Ping： ☑

禁止来自LAN口的Ping包通过路由器： ☑

保 存 帮 助 DoS 被禁主机列表

图 29 WAN 口 Ping

- 数据包统计时间间隔：该项设置对ICMP、UDP、TCP数据包进行统计的时间间隔，即在当前时间间隔内对各种数据包进行统计，如果统计得到的某种数据包(例如UDP FLOOD)达到了指定的阈值，那么系统将认为UDP-FLOOD 攻击已经发生，如果UDP-FLOOD过滤已经开启，那么路由器将会停止接收该类型的数据包,从而达到防范攻击的目的。
- DoS攻击防范：该项是开启下面各种攻击防范的总开关，只有选择此项后，以下的几种防范措施才能生效。
- 开启ICMP-FLOOD攻击过滤: 若需要防范ICMP-FLOOD攻击，请选择此项。
- ICMP-FLOOD数据包阈值：当开启ICMP-FLOOD功能后，如果在指定时间间隔内ICMP包达到了指定的数目，防范措施则立即启动。
- 开启UDP-FLOOD攻击过滤：若需要防范UDP-FLOOD，请选择此项。
- UDP-FLOOD数据包阈值：当开启UDP-FLOOD功能后，如果在指定时间间隔内UDP包达到了指定的数目，防范措施则立即启动。
- 开启TCP-SYN-FLOOD攻击过滤：若需要防范TCP-SYN-FLOOD，请选择此项。
- TCP-SYN-FLOOD数据包阈值：当开启TCP-SYN-FLOOD功能后，如果在指定时间间隔内TCP的SYN包达到了指定的数目，防范措施则立即启动。
- 忽略来自WAN口的Ping：若开启该功能，广域网的计算机将不能Ping通路由器。
- 禁止来自LAN口的Ping包通过路由器：若开启该功能，局域网的计算机将不能Ping通广域网中的计算机。
- DoS被禁主机列表：点击该按钮，你可以查看被禁止的主机列表，如图30。单击**刷新**按钮可以更新列表信息。若希望被禁主机能够重新上网，可以点击**删除**按钮；若需要释放所有被禁主机，可以点击**清空**按钮。



图 30 DoS 被禁主机列表

5.8 路由功能

选择菜单**路由功能**，您可以看到:

- 路由功能
  - 静态路由表

单击**静态路由表**，您即可进行静态路由功能设置，下面将详细讲解静态路由功能的设置。

5.8.1 静态路由表

选择菜单**路由功能→静态路由表**，您可以在下图31界面中设置的静态路由信息。

静态路由是一种特殊的路由，在网络中使用合适的静态路由可以减少路由选择问题和路由选择数据流的过载，提高数据包的转发速度。通过设定目的IP地址、子网掩码和网关地址可以确定一个路由条目，其中目的IP地址和子网掩码用来确定一个目标网络/主机，之后路由器会通过网关将数据包发往指定的目标网络/主机。

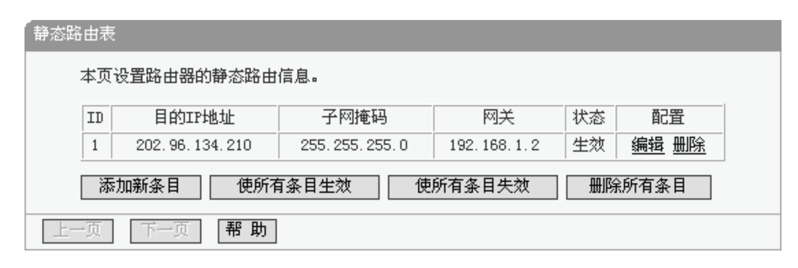


图 31 静态路由表

- 目的IP地址：用来标识希望访问的目标地址或目标网络。
- 子网掩码：该项与目的IP地址一起来标识目标网络，把目标地址和网络掩码逻辑与即可得到目标网络。
- 网关：数据包被发往的路由器或主机的IP地址。
- 状态：显示该条目是否生效，只有状态为生效时，此路由条目才起作用。
- 添加新条目：点击该项，你可以在下图中添加静态路由条目。如图32。

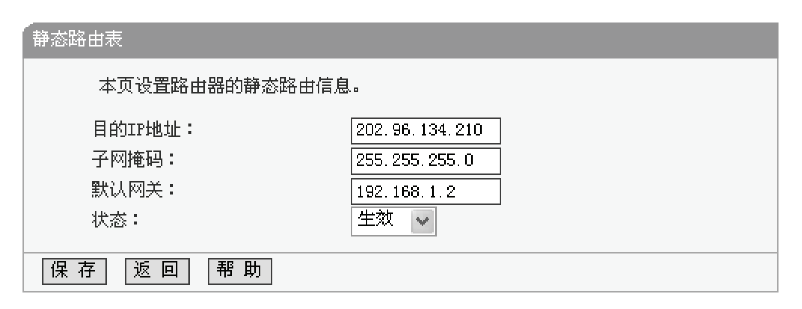


图 32 添加静态路由条目

完成设置后，点击**保存**按钮。

注意：

设置静态路由条目时，目的IP地址不能和路由器的WAN口或LAN口IP地址处于同一网段。

5.9 IP与MAC绑定

选择菜单**IP与MAC绑定**，您可以看到：

- IP与MAC绑定
  - 静态ARP绑定设置
  - ARP映射表

单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.9.1 静态ARP绑定设置

选择菜单**IP与MAC绑定→静态ARP绑定设置**，您可以在下图33界面中设置静态ARP绑定条目。

ARP绑定主要是将主机的IP地址与相应的MAC地址进行绑定，是防止ARP欺骗的有效方法。在路由器中设置静态ARP绑定条目，可以维护内网用户的上网安全。当主机向路由器发送ARP请求时，路由器会根据主机的IP地址去查看ARP静态绑定列表，若列表中的MAC地址与主机的MAC地址相同，则路由器会允许该ARP请求，否则将不允许该请求。

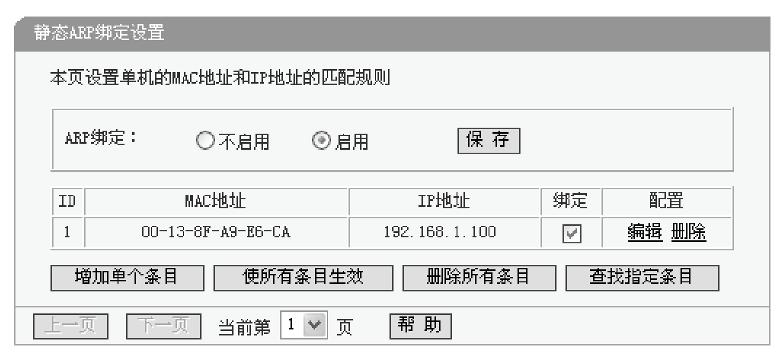


图 33 静态 ARP 绑定设置

- ARP绑定：该项用来开启ARP绑定功能，只有选择“启用”时，列表中的设置才能生效。
- MAC地址：该项显示被绑定主机的MAC地址。
- IP地址：该项显示被绑定主机的IP地址。
- 绑定：该项显示条目状态，只有选中该项，该条绑定条目才能生效。

例1：如果您希望将某台主机的IP地址和MAC地址进行绑定，其IP地址为192.168.1.100，MAC地址为00-13-8F-A9-E6-CA，这时您可以按照如下步骤设置:

第一步：在图33界面中点击**增加单个条目**。

第二步：在下图34中按照下图界面设置MAC地址和IP地址。

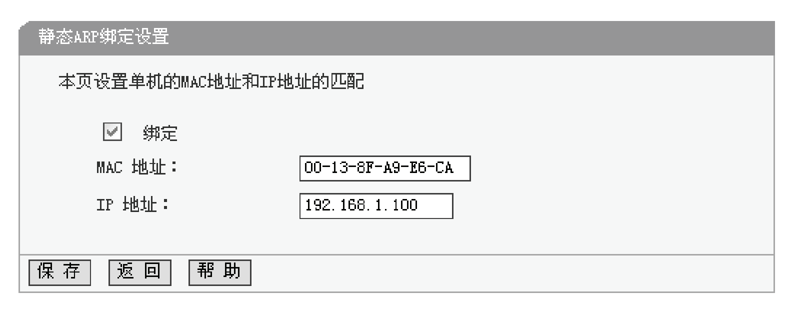


图 34 添加静态 ARP 绑定条目

第三步：设置完成后，选中“绑定”，并单击**保存**按钮。

5.9.2 ARP映射表

选择菜单**IP与MAC绑定→ARP映射表**，您可以在下图35图31界面中查看ARP绑定条目信息。


ARP映射表

ID	MAC地址	IP地址	状态	配置
1	00-13-8F-A9-E6-CA	192.168.1.100	已绑定	导入 删除

图 35 ARP 映射表

- 导入：该项用来将指定映射条目添加到静态ARP列表中(见图34)。
- 全部导入：该项用来将ARP映射列表中的所有条目添加到静态ARP列表中。
- 刷新：单击该按钮，您可以更新ARP映射列表中的条目信息。

注意：

1) 在进行导入操作时，如果该条目与ARP静态绑定表中的某条目冲突，则会显示冲突提示，不会添加该条目；
2) 在进行全部导入操作时，如果同样存在冲突条目，则系统会忽略冲突条目，将其它没有冲突的条目添加到ARP静态绑定列表中。

5.10 动态DNS

选择菜单**动态DNS**，您可以看到：

• 动态DNS

单击**动态DNS**，你可以进行相应的功能设置，下面将详细讲解动态DNS的功能。

动态DNS又名DDNS，它的主要功能是实现固定域名到动态IP地址之间的解析。对于使用动态IP地址的用户，在每次上网得到新的IP地址后，安装在主机上的动态域名软件就会将该IP地址发送到由DDNS服务商提供的动态域名解析服务器，并更新域名解析数据库。当Internet上的其他用户需要访问这个域名的时候，动态域名解析服务器就会返回正确的IP地址。这样，大多数不使用固定IP地址的用户，也可以通过动态域名解析服务经济、高效地构建自身的网络系统。

本路由器一共提供两种DDNS服务：花生壳DDNS、科迈网DDNS。花生壳DDNS的服务提供者是www.oray.net，科迈网DDNS服务提供者是www.comexe.cn。具体配置时，请首先选择您所需要的服务类型，即服务提供者。本路由器默认服务类型为花生壳DDNS。

1. 花生壳DDNS

选择服务提供者"花生壳(www.oray.net)"，您可以在下图36界面中设置DDNS。在注册成功后，可以用注册的用户名和密码登录到DDNS服务器上。当连接状态显示成功之后，互联网上的其它主机就可以通过域名的方式访问您的路由器或虚拟服务器了。

动态DNS设置

本页设置“Oray.net花生壳DDNS”的参数。

服务商链接：花生壳动态域名解析服务申请　花生壳动态域名解析服务帮助

服务提供者：花 生 壳 (www.oray.net)

用户名：

密 码：

启用DDNS：☑

连接状态：未连接

服务类型：- - -

域名信息：- - -

登 录　退 出

保 存　帮 助

图 36 花生壳 DDNS 设置

- 服务商链接：如果你还未在DDNS上注册，请选择该选项进行注册。
- 服务提供者：该项是提供DDNS的服务器。请根据需要选择所需的服务类型。
- 用户名、密码：请正确填写在DDNS上注册的用户名和密码。
- 启用DDNS：该项用来启用花生壳DDNS服务。
- 登录/退出：点击该按钮，您可以登录/退出DDNS服务。

2. 科迈网DDNS

选择服务提供者“科迈网(www.comexe.cn)”，您可以在下图37界面中设置DDNS。在注册成功后，可以用注册的用户名和密码登录到DDNS服务器上。当连接状态显示成功之后，互联网上的其它主机就可以通过域名的方式访问您的路由器或虚拟服务器了。

动态DNS设置

本页设置动态DNS参数

服务提供者： 科迈网（www.comexe.cn） 注册...
域名：
域名：
域名：
域名：
域名：

用户名：
密 码：

启用DDNS：
连接状态： 未连接

登 录 退 出

保 存 帮 助

图 37 科迈网 DDNS 设置

- 服务提供者：该项是提供DDNS的服务器。请根据需要选择所需的服务类型。若您还未在DDNS上注册，请选择"注册..."，您便可以登录服务器进行注册。
- 域名：该项是您在DDNS上注册的域名，请正确填写，可以填写多项。
- 用户名、密码：请正确填写在DDNS上注册的用户名和密码。
- 启用DDNS：该项用来启用科迈网DDNS服务。
- 登录/退出：点击该按钮，您可以登录/退出DDNS服务。

5.11系统工具

选择菜单**系统工具**，您可看到:

- 系统工具
  - 时间设置
  - 软件升级
  - 恢复出厂设置
  - 备份和载入配置
  - 重启路由器
  - 修改登录口令
  - 系统日志
  - 流量统计

单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.11.1 时间设置

选择菜单**系统工具→时间设置**，您可以在下图38界面中设置路由器的系统时间。您可以选择手动设置时间也可以选择从互联网上获取标准的GMT时间。

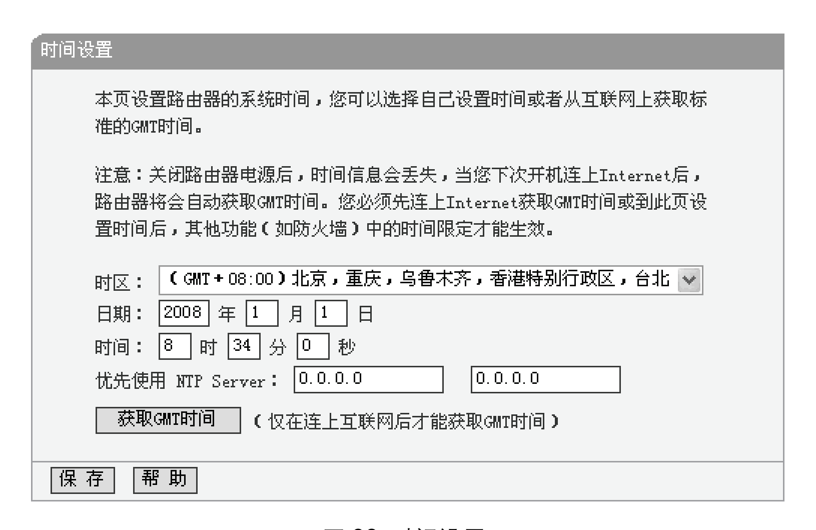


图 38 时间设置

➢ 优先使用NTP Server: 该项用来设置NTP Server的IP地址(最多可以输入两个)。NTP Server是网络时间服务器，用于互联网上的计算机时间同步。该路由器中内置了一些常用的NTP Server地址，一旦与Internet连接后，路由

器可以自动获取系统时间。但是，若此处设置了该项，则当路由器获取GMT时间时，将优先从已设置的时间服务器上获取。

时间设置步骤:

手动设置时间：首先请选择您所在的时区，然后在日期和时间栏内填入相应值，最后单击**保存**按钮即可完成系统时间的设置。

获取GMT时间：首先请连接互联网，然后选择您所在的时区，最后单击**获取GMT时间**按钮即可从互联网上获取标准的GMT时间。

⚠注意:

1) 关闭路由器电源后，时间信息会丢失，只有当您下次开机连上Internet后，路由器才会自动获取GMT时间。
2) 您必须先连上Internet获取GMT时间或在此页手动设置系统时间后，路由器其他功能(如防火墙)中的时间限定才能生效。
3) 当选择手动设置时间时，若要查看当前的系统时间，请刷新时间设置页面。

5.11.2 软件升级

选择菜单**系统工具→软件升级**，您可以在下图39界面中升级本路由器的软件版本。

软件升级

通过升级本路由器的软件，您将获得新的功能。

文件： [ ] 浏览...

当前软件版本： 3.6.1 Build 080311 Rel.34295na
当前硬件版本： FR524 1.0 1001225B

注意：升级时请选择与当前硬件版本一致的软件。升级过程需持续一段时间，在此期间不能关闭设备电源，否则将导致设备损坏而无法使用。当升级结束后，设备将会自动重新启动。

[升 级]

图 39 软件升级

软件升级步骤:

第一步：登录本公司的网站(www.fastcom.com.cn)，下载最新版本的软件。

第二步：在“文件”栏内填入已下载文件的全路径文件名，或用浏览按钮选择文件。

第三步：单击**升级**进行软件升级。

第四步：升级完成后，路由器将自动重启。

注意：

1) 升级时请选择与当前硬件版本一致的软件。升级过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。当升级结束后，路由器将会自动重启。

2) 软件升级后，路由器可能会恢复到出厂默认设置。

5.11.3 恢复出厂设置

选择菜单**系统工具→恢复出厂设置**，您可以将路由器的所有设置恢复到出厂时的默认状态。

恢复出厂设置后，路由器将自动重启，如图40。

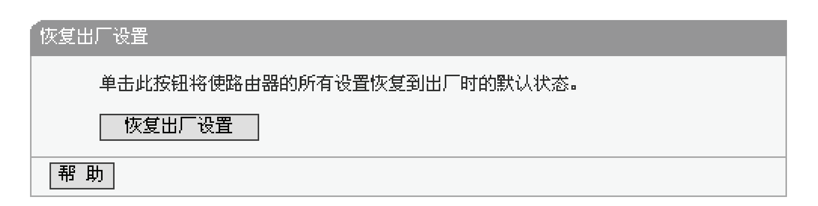


图 40 恢复出厂设置

单击**恢复出厂设置**按钮，路由器的所有设置将恢复到出厂时的默认状态。其中：

- 默认的用户名：admin
- 默认的密码：admin
- 默认的IP地址：192.168.1.1
- 默认的子网掩码：255.255.255.0

5.11.4 备份和载入配置

选择菜单**系统工具→备份和载入配置**，您可以在下图41中备份或载入路由器配置文件。

配置备份功能可以将路由器的设置以文件形式保存到电脑中，以备下次使用；在升级路由器软件或在载入新的配置文件前备份路由器的原有配置，可以有效防止升级软件或载入新配置文件过程中丢失原有配置的问题。

配置载入功能则可以将先前保存的或已编辑好的配置文件重新载入。如果需要为多台路由器配置相同的设置，则可以先配置一台路由器，保存其配置文件后，再将其载入到其它的路由器中，这样可以有效节省配置时间。

配置文件备份与载入

您可以在这保存您的设置。我们建议您在修改配置及升级软件前备份您的配置文件。

[备份配置文件]

您可以通过载入配置文件来恢复您的设置。

路 径： [ ] [浏览...] [载入配置文件]

注意： 1. 载入配置文件后，设备中原有的用户配置将会丢失，请先进行配置备份。如果您载入的配置文件有误，可能会导致设备无法管理和使用。
2. 载入配置文件的过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。载入文件的大小及配置命令正确与否会影响载入过程所需要的时间。如果载入结束且没有错误，路由器将会自动重新启动。

[帮 助]

图 41 配置文件备份与载入

例1: 如果您希望备份现有路由器的配置文件到C:\Router\backup，您可以按照如下步骤操作。

第一步：在图41界面中点击**备份配置文件**。

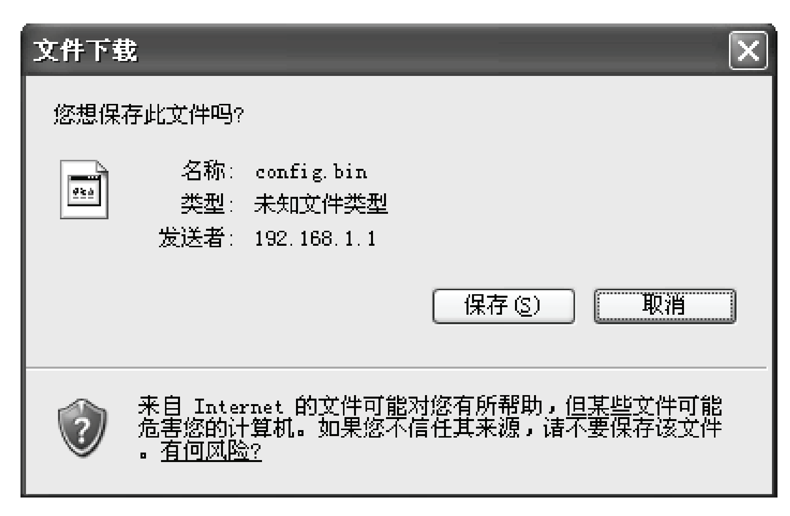


图 42 备份配置文件-文件下载

第二步：在图42界面中点击**保存**按钮。

第三步：在图43界面中选择文件存放路径“C:\Router\backup”，然后点击**保存**按钮即可完成文件备份。



图 43 备份配置文件-选择文件存放路径

例2: 如果您希望将C:\Router\backup目录下的config.bin文件载入到路由器中，您可以按照如下步骤操作。

第一步：在图41界面中输入文件的全路径“C:\Router\backup\config.bin”；此处也可以单击**浏览**按钮来选定该文件。

第二步：在图41界面中点击**载入配置文件**按钮。

注意:

1. 载入配置文件后，设备中原有的配置信息将会丢失，所以在导入配置文件前请先备份配置。如果您载入的配置文件有误，可重新载入先前备份的文件。
2. 配置文件载入的过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。载入文件的大小及配置命令正确与否会影响载入过程所需要的时间。如果载入结束且没有错误，路由器将会自动重新启动。如果载入有错，请根据提示信息自己选择是否保存配置，最好重启路由器。

5.11.5 重启路由器

选择菜单**系统工具→重启路由器**，您可以将路由器重新启动，如图44。



图 44 重启路由器

5.11.6 修改登录口令

选择菜单**系统工具→修改登录口令**，您可以在下图45界面中修改登录路由器管理界面的用户名和密码。修改时，需要先输入原用户名和原口令，然后再输入新用户名和新口令，如果您原来的用户名和口令输入无误的话，单击**保存**按钮即可成功修改用户名和口令。

修改登录口令

本页修改系统管理员的用户名及口令。

原用户名：admin

原口令：●●●●●

新用户名：user

新口令：●●●●●●

确认新口令：●●●●●●

保 存　清 空

图 45 修改登录口令

注意:

出于安全考虑，我们强烈推荐您更改初始系统管理员的用户名及密码。如果您忘了系统密码，请将路由器恢复到出厂设置。

5.11.7 系统日志

选择菜单**系统工具→系统日志**，您可以在下图46中查看路由器的日志信息。该界面记录了路由器的系统日志，您可以通过查询日志了解路由器上所发生的系统事件。单击**刷新**按钮，您可以更新日志内容，单击**清除所有日志**按钮，您可以删除当前所有的日志内容。

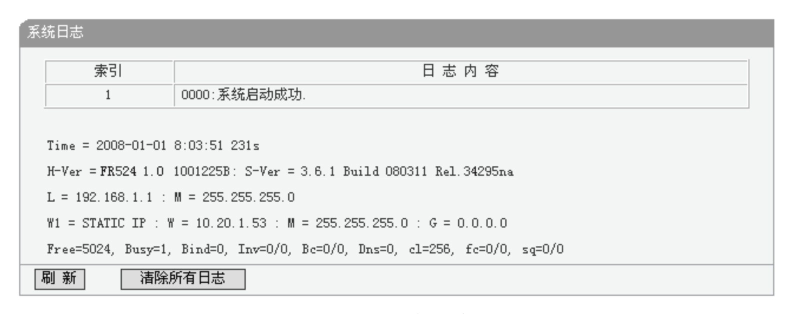


图 46 系统日志

5.11.8 流量统计

选择菜单**系统工具→流量统计**，您可以在下图47中查看路由器的流量信息。单击**刷新**按钮，您可以更新流量统计表；单击**重置**按钮，您可以重新设置统计粒度；单击**删除**按钮，您可以删除指定的流量统计信息。



图 47 流量统计

- 数据包统计时间间隔：该数值决定了统计路由器当前流量的时间间隔。它与**安全设置→高级安全设置**中的“数据包统计时间间隔”相同，无论在哪一个模块进行修改都会覆盖另一模块里的数值。因此在设置该值时，请注意两者的关联。
- IP地址：被统计主机的IP地址，此处也会显示该主机的MAC地址。
- 总流量：该项分别用数据包个数和字节数来统计路由器接收和发送数据的总流量。
- 当前流量：该项显示在不同的统计单位下，路由器在当前10秒钟内接收和发送不同数据的总流量。

注意：

1) *若要查看路由器的流量信息，必须先开启路由器的流量统计功能。如无需流量统计，可以关闭该功能，这样可以提高路由器的数据处理能力。*

2) *由于安全设置→高级安全设置中“DoS攻击防范”的部分功能是以相关数据包的统计为依据的，因此，如果流量统计功能被关闭，这部分功能也将失效。*

附录 A　FAQ

1、ADSL 用户如何设置上网?

1) 首先，将 ADSL modem 设置为桥模式（RFC1483 桥模式）。
2) 用网线将路由器的 WAN 口与 ADSL modem 相连, 电话线连 ADSL modem 的 Line 口。
3) 进入管理界面，选择菜单"网络参数"下的"WAN 口设置"，在右边主窗口中，"WAN 口连接类型"选择"PPPoE"，输入"上网帐号"及"上网口令"，点击连接按钮即可。
4) 如果是包月上网的用户，可以选择"自动连接"的连接模式；如果是非包月用户，可以选择"按需连接"或者"手动连接"，并且输入自动断线等待时间，防止忘记断线而浪费上网时间。

2、LAN 接入的用户如何设置上网?

1) 进入管理界面，选择菜单"网络参数"下的"WAN 口设置"，在右边主窗口中，"WAN 口连接类型"选择"动态 IP"，点击"保存"按钮即可。
2) 在某些网络服务商绑定了用户计算机网卡 MAC 地址的情况下，需要对路由器进行 MAC 地址克隆操作, 将路由器的 WAN 口 MAC 地址设置为被绑定的网卡 MAC 地址。选择菜单"网络参数"下的"MAC 地址克隆", 在右边主窗口中点击"克隆 MAC 地址"按钮，然后按"保存"按钮，待路由器重启动后生效。

3、怎样使用 NetMeeting 聊天?

1) 如果是主动发起 NetMeeting 连接，则不需要任何配置，直接在 NetMeeting 界面中输入对方的 IP 地址，即可进行 NetMeeting 呼叫。
2) 如果希望能接收来自对方的 NetMeeting 呼叫, 则需要设置虚拟服务器或 DMZ 主机。
3) 设置虚拟服务器方法：进入管理界面，选择菜单"转发规则"下的"虚拟服务器"，点击"添加新条目"按钮，在"服务端口号"栏填入"1720"（NetMeeting 的连接端口）,"IP 地址"栏填入您计算机的 IP 地址(假设您的 IP 地址是 192.168.1.100)，再在状态栏选择"生效"，点击"保存"按钮即可。如图:

虚拟服务器

虚拟服务器定义了广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过IP地址指定的局域网网络服务器。

服务端口号： 1720 (XX-XX or XX)

IP地址： 192.168.1.100

协议： ALL

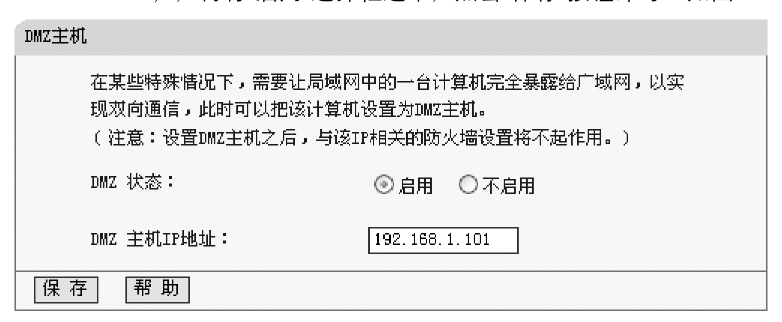
状态： 生效

常用服务端口号： --请选择--

保 存 返 回 帮 助

这样，对方呼叫您时只需输入您路由器 WAN 口的地址即可。

4) 设置 DMZ 主机方法：进入管理界面，选择菜单“转发规则”下的“DMZ 主机”，在“DMZ 主机 IP 地址”栏填入您计算机的 IP 地址（假设您的 IP 地址是 192.168.1.101），再将“启用”选择框选中，点击“保存”按钮即可。如图:



4 、怎样在局域网构建 Web 服务器?

1) 在局域网构建服务器，只需要按问题 3 的第三点设置虚拟服务器即可。

2) 但在构建 Web 服务器时，Web 服务的服务端口与路由器本身 Web 管理界面的缺省端口相同，都是 80，这样就引起冲突。解决办法是修改路由器 Web 管理界面的端口。

3) 进入管理界面，选择菜单“系统工具”下的“远端 Web 管理”，在右边主窗口中，“Web 管理端口”栏输入 80 以外的值，如 88。点击保存并重启路由器。如图:

远端WEB管理

本页设置路由器的WEB管理端口和广域网中可以执行远端WEB管理的计算机的IP地址。

注意： 1、路由器默认的WEB管理端口为80，如果您改变了默认的WEB管理端口（例如改为88），则您必须用“IP地址:端口”的方式（例如http://192.168.1.1:88）才能登录路由器执行WEB界面管理。此功能需要重启路由器才能生效。
2、路由器默认的远端WEB管理IP地址为0.0.0.0，在此默认状态下，广域网中所有计算机都不能登录路由器执行远端WEB管理，如果您改变了默认的远端WEB管理IP地址（例如改为202.96.12.8），则广域网中只有具有指定IP地址（例如202.96.12.8）的计算机才能登录路由器执行远端WEB管理。如果将远端WEB管理IP地址设为255.255.255.255，那么，广域网中所有的计算机都可以登录路由器执行远端WEB管理。

WEB管理端口： 88

远端WEB管理IP地址： 0.0.0.0

保 存 帮 助

4) 再次进入管理界面时，需要在浏览器的地址栏输入：http://192.168.1.1:88 才能进入。若远端用户需要访问该管理页面，必须输入 http://222.88.88.161:88（假设远端IP地址为 222.88.88.161）。

5) 进入管理界面，选择菜单“转发规则”下的“虚拟服务器”，点击“添加新条目”按钮，在“服务端口号”栏填入“80”，这是 Web 服务器的连接端口，“IP 地址”栏填入 Web 服务器的 IP 地址（假设您的 Web 服务器的 IP 地址是 192.168.1.100），再在状态栏选择“生效”，点击“保存”按钮即可。如图:

虚拟服务器

虚拟服务器定义了广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过IP地址指定的局域网网络服务器。

服务端口号： 80 (XX-XX or XX)

IP地址： 192.168.1.100

协议： ALL

状态： 生效

常用服务端口号： --请选择--

保 存 返 回 帮 助

附录 B　IE 浏览器设置

1. 打开 IE 浏览器，选择菜单工具→**Internet 选项(0)…**，如下图示。



2. 在 Internet 选项界面中选择**连接**，将“拨号和虚拟专用网络设置”中的设置内容全部删除(下图中该内容为空)，如下图示。



3. 选择**局域网设置(L)…**，按照下图界面所示进行配置。之后单击**确定**按钮返回。

局域网(LAN)设置

自动配置

自动配置会覆盖手动设置。要确保使用手动设置，请禁用自动配置。

☑ 自动检测设置(A)

☐ 使用自动配置脚本(S)

地址(R)

代理服务器

☐ 为 LAN 使用代理服务器(X) (这些设置不会应用于拨号或 VPN 连接)。

地址(E): 端口(T): 高级(C)...

☐ 对于本地地址不使用代理服务器(B)

确定 取消

4. 回到 IE 浏览器界面，选择菜单**工具→文件**，将下拉菜单中的脱机操作(W)取消(单击该项将前面的√去掉)，若该项没有启用，则不用设置。如下图示。

